FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA INDUSTRIAL

“IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA - 2021.”

Tesis para optar el título profesional de:

INGENIERA INDUSTRIAL

Autora:

Lucero Alessandra Arana Walde

Asesor:

Mg. Ing. Iselli Josylin Nohely Murga Gonzalez

Lima - Perú

2021

DEDICATORIA

Ante todo, darle gracias a Dios por darme sabiduría y entendimiento para desarrollarme en el trascurso de los años de mi ciclo académico, personal y profesional, porque sabemos que todos los que aman a Dios, todas las cosas les ayudan a bien; de la misma manera agradecer a mi familia quienes me han apoyado en todo momento, ya que gracias a su apoyo incondicional día a día puedo reponerme de las derrotas y así lograr celebrar juntos los triunfos.

AGRADECIMIENTO

A Dios por brindarme sabiduría para lograr desarrollar adecuadamente las asignaturas de la carrera. A mi madre, padre, familia y futuro esposo, por el esfuerzo y sacrificio que realizaron por brindarme los recursos necesarios para desarrollarme profesionalmente. A la Ing. Iselli Josylin Nohely Murga Gonzalez por el asesoramiento en el desarrollo de este presente trabajo de investigación.

TABLA DE CONTENIDOS

DEDICATORIA **2**

AGRADECIMIENTO **3**

ÍNDICE DE TABLAS **8**

ÍNDICE DE FIGURAS **9**

RESUMEN **10**

ABSTRACT **11**

I. CAPÍTULO. INTRODUCCIÓN **12**
I.1. Realidad problemática 12
I.2. Antecedentes 18
I.2.1. Antecedentes Internacional *18*
I.2.2. Antecedentes Nacionales *20*
I.2.3. Antecedentes Locales *21*
I.3. Marco teórico 23
I.3.1. Sistema de Gestión *23*
I.3.2. Sistema de Gestión de la Seguridad de la Información *24*
I.3.3. ISO 27001:2013 ..... *24*
I.3.4. Activo de información *26*
I.3.5. Información *26*
I.3.6. Análisis costo - beneficio *27*
I.3.7. Metodología MAGERIT *28*
I.3.8. Ciclo PHVA *29*
I.4. Justificación 30
I.5. Perspectiva de términos 32
I.6. Formulación del problema 33
I.7. Problemas específicos 33
I.8. Objetivos 33
I.8.1. Objetivo general *33*
I.8.2. Objetivos específicos *33*
I.9. Hipótesis 34
I.9.1. Hipótesis general *34*
I.9.2. Hipótesis especificas: *34*

II. CAPÍTULO. MÉTODO **36**
II.1. Tipo de investigación 36
II.1.1. Propósito *36*
II.1.2. Enfoque *36*
II.1.3. Diseño *36*
II.2. Población y muestra 37
II.2.1. Población. *37*

II.2.2. Muestra *37*
II.3. Técnicas, instrumentos y herramientas de recolección y análisis de datos 38
II.3.1. Técnicas *38*
II.3.1.1. La observación *38*
II.3.1.2. Revisión de documentos *38*
II.3.2. Instrumentos *38*
II.3.2.1. Matriz de consistencia *38*
II.3.2.2. Lista de verificación *39*
II.3.3. Herramientas *39*
II.3.3.1. Diagrama Gantt *39*
II.3.3.2. Matriz de riesgos de SI *39*
II.4. Procedimiento 41
II.4.1. Diagrama Gantt *43*
II.5. Método de análisis de datos 43
II.5.1. Validez *44*
Los 3 expertos fueron los siguientes: 44
II.5.2. Confiabilidad *44*
II.6. Aspectos Éticos 44

III. CAPÍTULO. RESULTADOS 45
III.1. Objetivo 1. Elaborar el diagnóstico de la empresa. 45
III.2. Objetivo 2. Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013. 47
III.3. Objetivo 3. Elaborar el análisis de riesgo de seguridad de la información 50
III.3.1. Planear *50*
III.3.1.1. Contexto de la organización *50*
III.3.1.1.1. Comprender la organización y su contexto 50
III.3.1.1.1.1. Misión 50
III.3.1.1.1.2. Visión 51
III.3.1.1.1.3. Foda 51
III.3.1.1.2. Comprender las necesidades y expectativas de las partes interesadas 53
III.3.1.1.3. Determinar el alcance del sistema de gestión 54
III.3.1.1.4. Sistema de gestión de seguridad de la información 54
III.3.1.2. Liderazgo *55*
III.3.1.2.1. Liderazgo y compromiso 55
III.3.1.2.2. Política 56
III.3.1.2.3. Roles, responsabilidades y autoridades organizacionales 58
III.3.1.3. Planificación *60*
III.3.1.3.1. Acciones para tratar los riesgos y las oportunidades 60
III.3.1.3.1.1. Generalidades 60
III.3.1.3.1.2. Valoración del riesgo de seguridad de la información 61
III.3.1.3.1.2.1. Valorización de activos de información 61
III.3.1.3.1.2.2. Análisis de riesgo 69

III.3.1.3.1.2.2.1. Identificación de Amenazas y vulnerabilidades 69
III.3.1.3.1.2.2.2. Cálculo de la Probabilidad 69
III.3.1.3.1.2.2.3. Cálculo del Impacto 70
III.3.1.3.1.2.2.4. Identificación de las Consecuencias 72
III.3.1.3.1.2.2.5. Cálculo del Nivel de Riesgo 72
III.3.1.3.1.2.3. Tratamiento del riesgo 72
III.3.1.3.1.2.3.1. Nivel de riesgo aceptable 72
III.3.1.3.1.2.3.2. Estrategias de tratamiento de riesgos 73
III.3.1.3.1.2.4. Selección de controles de seguridad 83
III.3.1.3.2. Objetivos de seguridad de la información y planificación para conseguirlos . 93
III.3.1.4. Soporte 94
III.3.1.4.1. Recursos 94
III.3.1.4.2. Competencia 94
III.3.1.4.3. Concientización 95
III.3.1.4.4. Comunicación 95
III.3.1.4.5. Información documentada 97
III.3.2. Hacer 98
III.3.2.1. Operación 98
III.3.2.1.1. Planificación y control operacional 98
III.3.2.1.2. Evaluación de riesgos de seguridad de la información 98
III.3.2.1.3. Tratamiento de riesgos de seguridad de la información 99
III.4. Objetivo 4. Evaluar el desempeño de la seguridad de información de la empresa CBC 99
III.4.1. Verificar 99
III.4.1.1. Evaluación del desempeño 99
III.4.1.1.1. Monitoreo, medición, análisis y evaluación 99
III.4.1.1.2. Auditoría interna 100
III.4.1.1.3. Revisión por la gerencia 101
III.4.2. Actuar 101
III.4.2.1. Mejora 101
III.4.2.1.1. No conformidades y acción correctiva 101
III.4.2.1.2. Mejora continua 102
III.5. O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013. 103

IV. CAPÍTULO. DISCUSIÓN Y CONCLUSIONES 104
IV.1. Alcance 104
IV.2. Limitaciones 104
IV.3. Interpretación comparativa 104

V. REFERENCIAS 112

VI. ANEXOS 117

VI.1. ANEXO 1. Matriz de consistencia 117
VI.2. ANEXO 2. Lista de Verificación 118
VI.3. ANEXO 3. Diagrama Gantt 124
VI.4. ANEXO 3. Diagrama Gantt 125
VI.5. ANEXO 3. Diagrama Gantt 126
VI.6. ANEXO 4. Lista de verificación de expertos 128
VI.7. ANEXO 5. Lista maestra 131
VI.8. ANEXO 6. Aplicabilidad 134
VI.9. ANEXO 7. FOR.002 Objetivos e indicadores 140
VI.10. ANEXO 8. POL.008 Caracterización de procesos 141
VI.11. ANEXO 9. FOR.003 Programa anual del SIG 143
VI.12. ANEXO 10. Acta de Comité 145
VI.13. ANEXO 11. Políticas de seguridad de la información 146
VI.14. ANEXO 12. MOF 151
VI.15. ANEXO 13. Rendición de cuentas 155
VI.16. ANEXO 14. Alcance 156
VI.17. ANEXO 15. Procedimiento de Gestión de riesgos y oportunidades 157
VI.18. ANEXO 16. Procedimiento de Gestión de activos 158
VI.19. ANEXO 17. Procedimiento de Gestión de riesgos SI 159
VI.20. ANEXO 18. Procedimiento de G.RRHH 160
VI.21. ANEXO 19. FOR.018 Evaluación del desempeño 161
VI.22. ANEXO 20. PRO.008 Capacitación 162
VI.23. ANEXO 21. Comunicaciones 163
VI.24. ANEXO 22. PRO.001 Control de información documentada 169
VI.25. ANEXO 23. PRO.004 Gestión de cambio 170
VI.26. ANEXO 24. PRO.015 Infraestructura Tecnológica 171
VI.27. ANEXO 25. PRO.003 Gestión de auditoria 172
VI.28. ANEXO 26. FOR.009 Programa anual de auditoria 173
VI.29. ANEXO 27. PRO.011 Gestión de Proveedores 174
ANEXO 28. PRO.007 Revisión por la direcció 175
VI.30. ANEXO 29. PRO.002 Tratamiento de NC y acción correctiva 176
VI.31. ANEXO 30. FOR.007 Registro de Acciones correctiva 177
VI.32. ANEXO 30. Verificación de Controles SI 178

ÍNDICE DE TABLAS

Tabla 1 Organizaciones Internacionales certificadas con la ISO 27001:2013 13
Tabla 2 *Organizaciones nacionales certificadas con la ISO 27001:2013* 16
Tabla 3 *Técnicas, instrumentos y herramientas de recolección y análisis de datos* 40
Tabla 4 *Procedimiento* 41
Tabla 5 *Calificación del Check list* 45
Tabla 6 *Cumplimiento de la norma ISO 27001:2013 antes de la implementación* 46
Tabla 7 *Costos de RRHH* 47
Tabla 8 *Costo Total según su tipo* 48
Tabla 9 *Beneficio* 49
Tabla 10 *Costo/beneficio* 49
Tabla 11 *Partes interesadas y requisitos* 53
Tabla 12 *Valoración de activo* 62
Tabla 13 *Inventario de Activos* 63
Tabla 14 *Inventario de Activos* 64
Tabla 15 *Inventario de Activos* 65
Tabla 16 *Inventario de Activos* 66
Tabla 17 *Inventario de Activos* 67
Tabla 18 *Inventario de Activos* 68
Tabla 19 *Valor del activo* 69
Tabla 20 *Probabilidad del riesgo* 70
Tabla 21 *Impacto del riesgo* 71
Tabla 22 *Matriz de riesgo* 74
Tabla 23 *Matriz de riesgo* 75
Tabla 24 *Matriz de riesgo* 76
Tabla 25 *Matriz de riesgo* 77
Tabla 26 *Matriz de riesgo* 78
Tabla 27 *Matriz de riesgo* 79
Tabla 28 *Matriz de riesgo* 80
Tabla 29 *Matriz de riesgo* 81
Tabla 30 *Matriz de riesgo* 82
Tabla 31 *Tratamiento SI* 84
Tabla 32 *Objetivos* 93
Tabla 33 *Cumplimiento de la implementación* 103

ÍNDICE DE FIGURAS

Figura 1 Certificación de la ISO 27001:2013 13
Figura 2 Denuncias recibidas en la DIVINDAT (2015-abril 2021) 15
Figura 3 Denuncias recibidas en la DIVINDAT de enero a abril 2021 15
Figura 4 Certificación ISO 27001:2013 16
Figura 5 Foda 52
Figura 6 Mapa de proceso 54
Figura 7 Política de excelencia organizacional 57
Figura 8 Organigrama 58
Figura 9 Nivel de riesgo 72
Figura 10 Formato de Plan anual de capacitaciones 95
Figura 11 Programa de comunicaciones y sensibilización interna 96
Figura 12 Lista de Verificación 118
Figura 13 Diagrama de Gantt 124
Figura 14 Lista de verificación de expertos 128
Figura 15 Lista maestra 131
Figura 16 Aplicabilidad 134
Figura 17 Objetivos e indicadores de CBC 140
Figura 18 Caracterización de procesos 141
Figura 19 Programa anual 2021 143
Figura 20 Acta de Comité 145
Figura 21 Políticas de Seguridad de la Información 146
Figura 22 *Manual de organización y funciones* 151
Figura 23 Rendición de cuentas 155
Figura 24 Alcance 156
Figura 25 Procedimiento de Gestión de riesgos y oportunidades 157
Figura 26 Procedimiento de Gestión de Activos 158
Figura 27 Gestión de riesgos operacionales de SI 159
Figura 28 Gestión de RRHH 160
Figura 29 Evaluación del desempeño 161
Figura 30 Procedimiento de Capacitación 162
Figura 31 Comunicaciones SI 163
Figura 32 Procedimiento de Control de información documentada 169
Figura 33 Procedimiento de Gestión de Cambio 170
Figura 34 Procedimiento Infraestructura Tecnológica 171
Figura 35 Procedimiento de Gestión de Auditoria 172
Figura 36 Programa de auditoria 27001:2013 173
Figura 37 Gestión de proveedores 174
Figura 38 Revisión por la dirección 175
Figura 39 Tratamiento de NC y AC 176
Figura 40 Registro de AC 177
Figura 41 Controles SI 178

RESUMEN

La presente investigación tiene como objetivo general implementar el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 en la empresa Core Business Corp. SAC para proteger la información en los procesos Operativos. Asimismo, se hizo uso de las técnicas de observación y revisión documentada, el instrumento usado fue la lista de verificación para comprobar el cumplimiento de la norma ISO 27001:2013 y matriz de consistencia, además, se usaron las herramientas de diagrama Gantt y matriz de riesgos con la finalidad de dar respuesta a los objetivos de la presente investigación. La metodología usada fue el ciclo PHVA y MAGERIT permitiendo lograr la implementación. Como resultado, se obtuvo en el diagnostico organizacional un 38 % de cumplimiento, desarrollándose la implementación de la norma ISO 27001:2013, culminando así con un 100%. Además, al costo/beneficio fue de 1.96, siendo el beneficio mayor al costo y por ende la implementación es rentable para Core Business. En conclusión, la implementación permite proteger los activos de información mediante los controles definidos al realizar el análisis de riesgos de SI dentro del capítulo 6.1.3 de la norma ISO 27001:2013, además de contar con beneficios que permiten dar cumpliendo con los objetivos de la presente investigación.

Palabras clave: Norma ISO 27001:2013, cumplimiento, lista de verificación, matriz de riesgos, activos de información.

ABSTRACT

The general objective of this is to implement the information security management system based on ISO 27001: 2013 in the company Core Business Corp. SAC to protect information in Operational processes, thus we respond to the problem. Likewise, observation and documented review techniques were used, the instrument used was the checklist to verify compliance with the ISO 27001: 2013 standard and consistency matrix, in addition, the Gantt chart and matrix tools were used. risks in order to respond to the objectives of this research. Likewise, the PHVA and MAGERIT metodología is used, allowing implementation to be achieved. As a result, 38% compliance was obtained in the organizational diagnosis, developing the implementation of the ISO 27001: 2013 standard, thus culminating with 100%. In addition, the cost / benefit was 1.96, the benefit being greater than the cost and therefore the implementation is profitable for Core Business. In conclusion, the implementation allows the protection of information assets through the controls defined when carrying out the IS risk analysis within chapter 6.1.3 of the ISO 27001: 2013 standard, in addition to having benefits that allow us to comply with the objectives of the present investigation.

Keywords: ISO 27001: 2013 Standard, compliance, checklist, risk matrix, information assets.

I. CAPÍTULO. INTRODUCCIÓN

I.1. Realidad problemática

Existen diversas amenazas que pueden perjudicar a una organización, como el acceso a la red o al sistema de información por personas no autorizadas, incumplimiento de relaciones contractuales con el cliente o partes interesadas, infracción legal, comprometer información confidencial, fuga de información debido al termino de contrato y errores de software, entre otros.

Por ello, la información, los sistemas informáticos y procesos forman activos de información que la organización debería mantener adecuadamente, minimizando los riesgos que tendrían estos al no contar con controles.

A nivel mundial, los robos cibernéticos y/o ciberdelincuencia son una forma de delincuencia transnacional y uno de los que crecen cada año, este delito afecta a más de 431 millones de víctimas adultas a nivel mundial. (Norton, 2012)

El uso de software malicioso y suplantación de páginas web es el delito que más se presenta, pero también se cuenta con robo de la identidad, el malware (software instalado involuntariamente que recoge información personal) y hacking (acceso ilegal a la computadora de alguien de forma remota) corroborando lo mencionado por la empresa Sistemius (2020) mencionando que: este delito atenta a la confidencialidad, integridad y disponibilidad de los sistemas informáticos de una organización.

Actualmente, muchas organizaciones han optado por implementar la ISO 27001:2013 y por ende certificarse, pero se debe tener en cuenta que la implementación y certificación de la norma ISO 27001 puede tardar entre 4 o 6 meses en una empresa pequeña, pero en algunos casos puede tardar 12 meses debido a que no se tiene alguna persona con experiencia en

implementación ISO 27001:2013, en el caso de una organización de tamaño mediano tardaría hasta 10 meses y para una organización grande 1 año. (Iso Tools, 2017)

Tomando en cuenta ello, a nivel mundial las siguientes organizaciones cuenta con certificación:

Tabla 1

Organizaciones Internacionales certificadas con la ISO 27001:2013

Ámbito	Organización Certificada
SGSI Internacionales	Microsoft Global Foundation Services (GFS), Google Apps, Amazon Web Services (AWS), IFX Networks Colombia, EQUIFAX Chile.

Adaptado de la tesis Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la iso/iec 27001:2013, para una empresa de consultoría de software de los autores. Llanos & Elías (2016)

De acuerdo, a la ISO en el año 2019 y 2020 se ha incrementado en todo el mundo la implementación y por ende la certificación de la ISO 27001:2013 (ver figura 1). (ISO,2020)

Figura 1

Certificación de la ISO 27001:2013

Para la figura 1 se utilizó algunos países de Sudamérica, Asia y Europa para visualizar el crecimiento a nivel mundial. (ISO,2020)

En una sociedad cada vez más digitalizada y ante las nuevas necesidades que han surgido a raíz de la crisis sanitaria COVID-19, también se ha desarrollado el espionaje industrial, dando lugar a situaciones comprometedoras para las empresas, ya sean pequeñas corporaciones o grandes multinacionales.

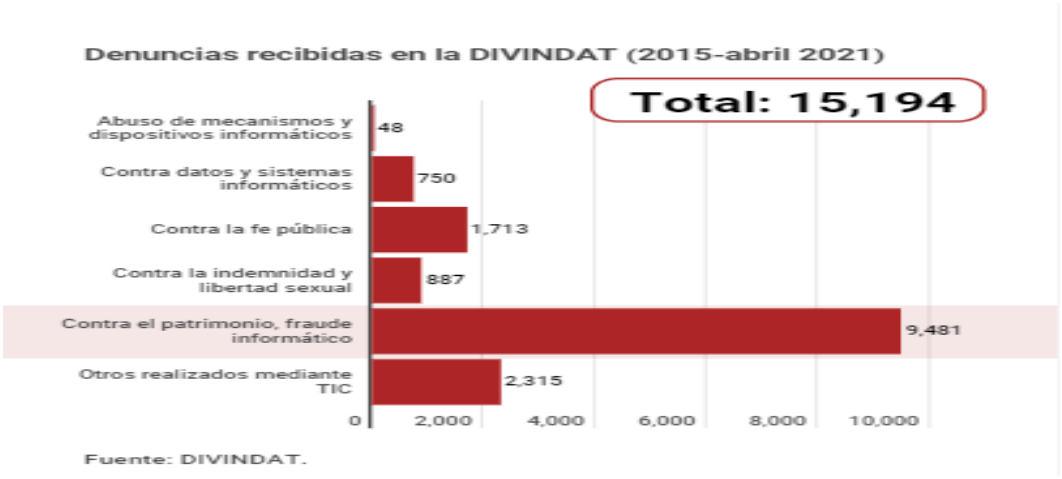
Asimismo, PwC Perú, declaro que el uso de herramientas de ciberacoso y espionaje ha aumentado un 145% en el 2020 en adelante. (Gascón, 2021)

Además, la fuga de información es una amenaza para las empresas, ya que estas pierden más dinero, reputación y prestigio. En el año 2013, el 70% de las PYMES sufrió fugas de datos de modo accidental o intencional, en ambos casos pudiendo ser provocadas por parte de sus trabajadores o resultado de un ataque dirigido.(América Economía, 2014)

Entre enero y abril del 2021 en el Perú, se investigaron 1,188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía. Los casos más frecuentes desde el año 2015 hasta la actualidad están relacionados al fraude informático y a la suplantación de identidad (Ver figura 2 y 3).

Figura 2

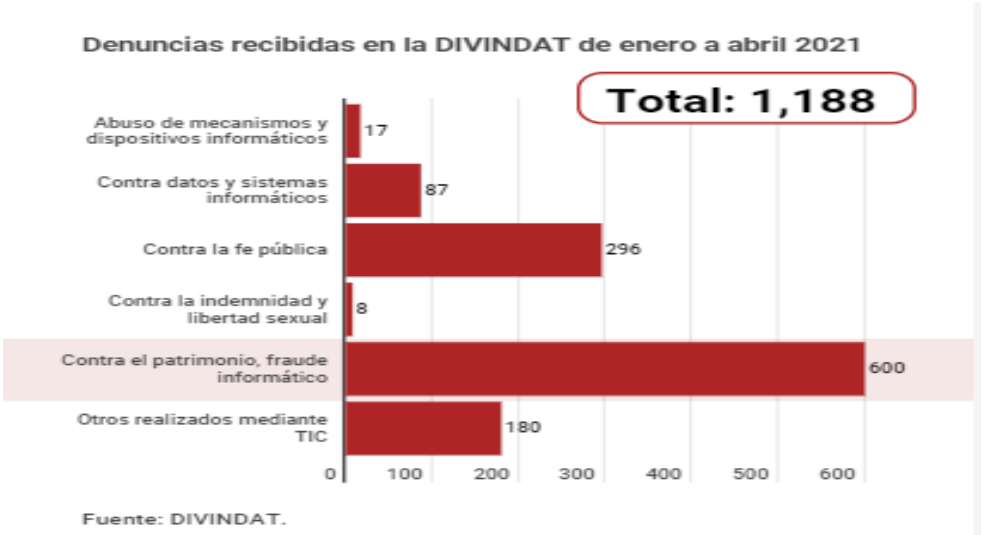
Denuncias recibidas en la DIVINDAT (2015-abril 2021)



El grafico representa las denuncias recibidas en la DIVIDAT desde el año 2015 hasta abril del 2021, en el cual se evidencia que la denuncia con mayor incidencia es contra el patrimonio, fraude informático. Fuente: Divindat.

Figura 3

Denuncias recibidas en la DIVINDAT de enero a abril 2021



El grafico representa las denuncias recibidas en la DIVIDAT en el mes de enero a abril del 2021, en el cual se evidencia 1188 denuncias en total. Fuente: Divindat.

Asimismo, en Perú muchas organizaciones han adoptado por implementar la ISO 27001:2013, así como:

Tabla 2

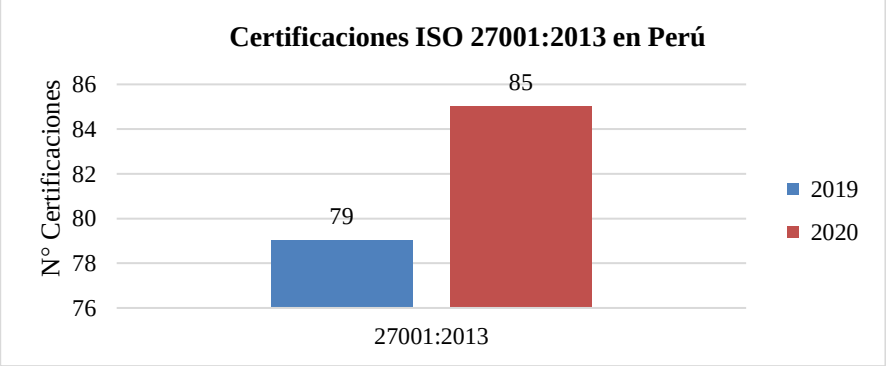
Organizaciones nacionales certificadas con la ISO 27001:2013

Ámbito	Organización Certificada
SGSI Nacionales Sector Público	Oficina de Normalización Previsional (ONP), Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN), Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), Banco Central de Reserva del Perú (BCRP), Instituto Nacional de Defensa de La Competencia y de La Protección de La Propiedad Intelectual (INDECOPI), Superintendencia de Mercado de Valores (SMV)
SGSI Nacionales Sector Privado	Bolsa de Valores de Lima (BVL), Grupo Graña y Montero (GMD), RIMAC Seguros, Hermes, Compañía Minera Hochscild, Terra (Media Network), Atento Perú, T-Gestiona, Telefónica Empresas, Telefónica del Perú, PMC Latam, Soluciones Orión.

Fuente: Adaptado de la tesis de los autores Llanos & Elías (2016), ya que al buscar evidencia de cada empresa se concluyó que si contaban con la certificación mencionada.

Figura 4

Certificación ISO 27001:2013



Se evidencia que en el Perú se cuenta con un incremento de 6 empresas certificadas en el año 2020 respecto al año anterior 2019.

La seguridad de la información basado en la norma ISO 27001:2013 consiste en preservar la confidencialidad de esta, así como su integridad y disponibilidad, permite mejorar la imagen de la organización y el aumento de prestigio, ya que brinda una mayor confianza por parte de clientes, proveedores, accionistas y socios, ayuda a la organización a gestionar y proteger la información, así como a conocer los posibles riesgos para establecer las medidas de seguridad necesarias, y disponer de control para disminuir los riesgos que tienen los activos de información.(Javier, 2008)

Entre los activos más importantes de una organización está la información tanto en los procesos, como en los activos que cuentan con dicha información y, por tanto, la custodia (usuario) de esta es un factor relevante para su continuidad y éxito profesional.

Core Business Corp. cuenta con la ISO 9001:2015 y si bien esta le permite mantener controles que satisfacen a sus clientes mediante la calidad de servicio que brindan, dentro de la presente investigación no se evidencio un adecuado sistema de seguridad de la información que permita asegurar la confidencialidad, integridad y disponibilidad de la los activos de información dentro de sus procesos operativos. Por un lado, los propios clientes solicitan y/o consultan si se cuente con la ISO 27001 ya que este brinda prestigio, confianza, compromiso entre otros beneficios, al no tenerlo muchos clientes no culminan con un acuerdo. Por otro lado, el desconocimiento de una política de seguridad, el mal uso de las tecnologías de la información y falta de controles perjudican a la organización generando riesgos e incumplimientos de acuerdos de clientes que se evitaría si contaran con un sistema de gestión de seguridad de la información.

En relación con lo descrito anteriormente, se realizó esta investigación a fin de dar respuesta a: ¿De qué manera la implementación del Sistema de Gestión de la Seguridad de la

Información ISO 27001:2013 en la empresa Core Business permite proteger la información de los procesos Operativos?

Con ello, se tiene como objetivo general implementar el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 en la empresa Core Business Corp. SAC para proteger la información en los procesos Operativos.

I.2. Antecedentes

El presente estudio posee diversos antecedentes los cuales han servido como marco referente para la elaboración del marco teórico y prácticas del presente trabajo, a continuación, los antecedentes que se ajustaron a las variables.

I.2.1. Antecedentes Internacional

Yagual del Valle y Rodríguez (2014), en su tesis titulada "Análisis para la integración de un sistema de Gestión de Seguridad de Información (SGSI) ISO 27001 utilizando OSSIM para empresa industrial". Estableció como objetivo minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la ISO 27001 combinando las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área de Tecnología de información. Asimismo, las técnicas e instrumentos utilizados fueron la entrevista, encuesta y observación. La metodología usada según su propósito es exploratorio, cualitativo y descriptivo. Asimismo, el método de investigación de riesgo usado fue el de Magerit, el cual permitió realizar la matriz de riesgo para cada proceso, determinando que tan expuesto se encontraba un activo de información. La población estuvo constituida por los integrantes de la empresa. En conclusión, se identificaron 15 riesgos que podrían afectar a 18 procesos críticos, para cada riesgo se seleccionaron los controles adecuados referentes a la norma ISO 27001, explicando

su objetivo y control a seguir proponiéndose de tal forma un plan de contingencia en el área TI.

Torres (2020), en su tesis titulada "Plan de Seguridad Informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A". Estableció como objetivo elaborar una propuesta de plan de seguridad informática utilizando la norma ISO 27001 en dicha empresa. Asimismo, las técnicas e instrumentos utilizados fueron la entrevista y encuesta personal. La metodología usada fue según su propósito aplicada y enfoque cualitativo, ya que se requiere la recolección de la información para tener un análisis completo de la actual situación de la empresa. Se tomó como población al personal integrado por cuatro personas en el departamento de Tics de la empresa ,asimismo, no es necesario realizar un muestreo debido a que la población es reducida y se puede acceder a ella sin restricciones. En conclusión, se tomó conciencia sobre la importancia que tiene la seguridad de la información en la actualidad, ya que se debe contar un Sistema de Gestión de la Seguridad de la información aplicado mediante la norma internacional ISO 27001, además, fue de vital importancia contar con una matriz de riesgos, la cual ayudo a identificar las vulnerabilidades existentes en los activos de información, el cual se desarrolló gracias a la metodología MAGERIT permitiendo identificar la probabilidad e impacto de riesgos a los que se pueden enfrentar los activos de información, para poder emplear los controles necesarios para mitigar los riesgos existentes.

Córdoba (2021), en su tesis titulada "Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia". Estableció como objetivo diseñar un sistema automatizado de gestión de la seguridad de la información basado en la Norma

ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 26 2012 de protección de datos personales en el Departamento de Sistemas de una institución universitaria en Colombia. Asimismo, las técnicas fueron la observación y el instrumento utilizado fue la lista de chequeo que permitió evaluar el nivel de cumplimiento tras la implementación de un SGSI, se identificó el riesgo de acuerdo con las escalas de probabilidad e impacto atendiendo a la Norma ISO 27001 y el cumplimiento de la Ley 1581 de 2012. La metodología usada según su propósito es aplicada y diseño experimental. La población para la presente investigación es la institución universitaria de carácter privado, asimismo, la muestra es el departamento de sistema. En conclusión, la identificación de los requerimientos que exige la Norma ISO 27001:2013 y la Ley 1581 sirvieron de contexto para analizar la totalidad de las exigencias que promueven el cumplimiento frente la protección de datos personales, la cual aplica para instituciones públicas y privadas a nivel nacional, también alerta sobre los riesgos administrativos y económicos que conllevaría para la institución universitaria el no cumplimiento, así puede llevarse a cabo de diferentes formas y recursos, aquí se privilegió el logro de un objetivo a bajo costo, no obstante, el resultado fue posible gracias a la integración de una mirada sistémica que incluyó una ley, una norma y una plataforma de automatización.

I.2.2. Antecedentes Nacionales

Vilca (2017), en su tesis titulada “Diseño e Implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de lima”. Estableció como objetivo determinar la mejora de implementación de un sistema de gestión de seguridad de la información para la seguridad del área de recursos humanos de la empresa GEOSURVEY S.A. Asimismo, las técnicas e instrumentos utilizados fueron el cuestionario de encuesta, con el propósito de recolectar toda la información de los

trabajadores de las diferentes áreas de la empresa GEOSURVEY S.A, relevante con respecto a la seguridad de la información de dicha empresa. La metodología usada es de enfoque cuantitativo asimismo su diseño es pre experimental de pre y post prueba en el grupo de la investigación. La población estuvo constituida por los integrantes del órgano administrativo y operativo de la empresa, en este caso se consideraría a todos aquellos como la muestra representativa ya que la cantidad de trabajadores por área es mínima. En conclusión, se logró optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa, al uso de los equipos de la empresa, al uso de la información en la empresa GEOSURVEY tras la intervención la cual permitió una mejora del sistema de gestión de seguridad de la información en su área de Recursos Humanos.

I.2.3. Antecedentes Locales

Llanos y Elías (2016), en su tesis titulada "Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software". Estableció como objetivo desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013. En conclusión, se elaboró una implementación y se cumplido los requisitos del estándar 27001 donde se consideraron aquellos estándares que forman parte del dominio de algunos de los requisitos del SGSI, además, como resultado de las exigencias del proyecto y sus interesados, se elaboraron propuestas innovadoras asociadas a: la metodología de gestión de riesgos, la normalización de los planes del sistema y realizar la verificación integral de cumplimiento de los componentes requeridos como requisitos por la ISO/IEC 27001:2013.

Vásquez (2018), en su tesis titulada "Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI". Estableció como objetivo Implementar el sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. La metodología empleada es de tipo de investigación descriptiva aplicada. Además, su tipo de investigación responde a un Diseño experimental. La población y muestra para esta investigación fue de 56 personas. Además, se hizo uso de las técnicas de encuestas, análisis documentario y auditorias. En conclusión, el autor menciona que la norma ISO 27001:2013 puede integrarse a las diversas normas debido a su estructura a las demás normas ISO 9001, ISO 14000, etc., asimismo, debido a que el personal es un factor importante y es quien opera en su mayoría los procesos del negocio, es necesario que esté capacitado en temas técnicos para la operación del proyecto y concientizado en la importancia de la seguridad de la información y en que sus actividades contribuyen a la protección de la información.

Benites (2019), en su tesis titulada "Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza". Estableció como objetivo implementar un Sistema de Gestión de Seguridad de la información en la Oficina de Proyectos que se encuentra dentro de Área de Planta en la fábrica de Radiadores Fortaleza. La metodología empleada es de tipo de investigación es documental-correlacional. Además, su tipo de investigación responde a un Diseño experimental. La población para esta investigación fueron todo el personal de dibujo mecánico del área de planta y las jefaturas de la Fábrica de Radiadores Fortaleza, desde el puesto más alto hasta cada uno de los empleados y la muestra fueron todos los encargados principales (Gerentes, jefes) de todas las áreas de la Fábrica de Radiadores Fortaleza, el personal del área de Tecnologías de Información encargados de llevar a cabo la aplicación de las políticas a nivel

técnico y administrativo y los dibujantes mecánicos de la Fábrica de Radiadores Fortaleza. Además, los instrumentos de recolección de datos fueron cuestionarios y entrevistas. En conclusión, el desarrollo del plan de Implementación de un SGSI requiere de un minucioso trabajo, esfuerzo y gran desempeño de toda la Fábrica de Radiadores Fortaleza, asimismo, la ejecución de los controles, políticas, metodologías y estrategias planteadas en el desarrollo del SGSI viene acompañada del compromiso de los jefes de cada área ya que son los responsables del resultado del SGSI, además, la generación de controles informáticos genero un buen impacto en el resguardo de los activos de información, las pruebas de ellos se demostraron. El resultado fue satisfactorio, se redujo considerablemente los incidentes técnicos, así como la reducción de tiempo de respuesta en el usuario y en el responsable de TI, gracias a esto se afianzo la seguridad y confianza del usuario del área TI.

I.3. Marco teórico

Para esta investigación es necesario el fundamento teórico para profundizar en el conocimiento eficiente relacionado a las variables.

Por ello, con el fin de obtener una mejor comprensión del problema de investigación, se presentan un conjunto de conceptos. Dada que los siguientes bases teóricas permiten sostener el desarrollo del trabajo. En ese sentido, se consideran las siguientes bases teóricas descritas a continuación:

I.3.1. Sistema de Gestión

El sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. Este incluye la estructura organizativa, políticas, planificación de actividades,

responsabilidades, prácticas, procedimientos, procesos y recursos que permiten en su conjunto planificar, controlar, organizar y automatizar cada actividad.(ISO, 2020)

I.3.2. Sistema de Gestión de la Seguridad de la Información

La ISO 27001:2013 define el sistema de gestión de la seguridad de la información como el preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos. Asimismo, de acuerdo a la ISO 27000:2014 define la confidencialidad como propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados, así como la integridad como la propiedad de la información de exactitud y completitud, y, la disponibilidad como propiedad de la información de ser accesible o usable cuando sea demandada por una entidad autorizada. De tal modo que se debe tener claro que es un riesgo, siendo este un efecto que genera incertidumbre sobre el logro de los objetivos de seguridad de información y la amenaza es la causa potencial de un incidente inesperado, que podría resultar un daño a un sistema o a la organización.

I.3.3. ISO 27001:2013

ISO 27001:2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada el 2013 y ahora su nombre completo es ISO/IEC 27001:2013. (ISO 27001)

ISO/IEC 27001:2013 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias y estas no son un requisito para la implementación, mientras que las secciones del 4 a 10 son requisitos, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Además, los controles del Anexo A

deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Esto se realiza investigando cuáles son los principales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

I.3.4. Activo de información

El activo de Información es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos, y por lo tanto tiene valor para la organización. (Dirección General de Modernización Administrativa, 2012)

Además, los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.(Niño, 2018)

La información puede ser almacenada en muchas formas, incluyendo: forma digital como en archivos de datos almacenados en medios electrónicos, forma material como documentación, discos duros entre otros, así como la información está en el conocimiento de los colaboradores. La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal. De modo que siempre se necesita una protección conveniente. (Llanos y Elías, 2016)

También, el activo de información cuenta con un propietario del Riesgo, este es la persona o entidad con la capacidad y autoridad para gestionar el riesgo.

I.3.5. Información

La información es un conjunto de datos organizados en poder de una entidad que posee valor de la misma, independientemente de la forma en que se guarde o transmita de su origen o de la fecha de elaboración. Este es un recurso vital para toda organización, y el buen uso de ésta puede significar la diferencia entre el éxito o el fracaso para una organización. Este tiene un ciclo de vida el cual es creada, guardada, destruida y utilizada.

Además, esta se clasifica en publica, en la cual todos los colaboradores de una organización tienen acceso a la información, interna, solo es de uso para la organización y confidencial es la información estricta para un grupo de personas dentro de una organización. (Fonquernie, 2015)

I.3.6. Análisis costo - beneficio

El análisis del costo-beneficio se refiere a la evaluación de un determinado proyecto, de un esquema para tomar decisiones de cualquier tipo. Por lo tanto, se determina el total de costos y beneficios de todas las alternativas para seleccionar la mejor o más rentable. Este análisis se deriva de la unión de diversas técnicas de gerencia y de finanzas, que presentan tanto los costos como los beneficios en unidades de medición estándar usualmente monetarias para que se puedan comparar directamente.(Aguilera, 2017)

En donde:

Si B/C > 1 , Se acepta.

Si B/C = 1 , Indiferente.

Si B/C < 1 , Se rechaza.

Navarro y Malta (2016), menciona que los beneficios internos se refieren a una mayor iniciativa y capacidad de liderazgo por parte de la dirección, incremento en la consistencia de las operaciones, la mejora continua de procesos y productos. Además, esta se asocia a la reducción de costes, una mayor opción para alcanzar una certificación ISO y la mejora en la gestión administrativa.

Asimismo, el mismo autor describe que los beneficios externos se encuentran relacionados a la mejora en la satisfacción de los clientes, la posición competitiva, las

comunicaciones externas, la reputación e imagen, mayor flexibilidad en los procesos operativos y la disminución de los reclamos por parte de los clientes.

También, menciona que se cuenta con un costo principal el cual está relacionada a las actividades de implementación del sistemas de gestión pertinente.

I.3.7. Metodología MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), se basa en el estudio de los activos de información relevantes para el negocio, considerándose los puntos de vista: cualitativo y cuantitativo. (Pae, 2012)

El siguiente proceso, es el esquema general de la metodología:

- Determinar los activos, subgrupos y/o grupos de activos de información relevantes para la organización, su interrelación y su valor, en el sentido de qué costo asumiría la organización al sufrir su pérdida.
- Determinar las amenazas sobre los objetivos del negocio, en términos de confidencialidad, integridad y disponibilidad de la información.
- Determinar las posibles consecuencias.
- Determinar la probabilidad de ocurrencia del evento potencial.
- Estimar el nivel de impacto que dependerá de la confidencialidad, integridad y disponibilidad.
- Estimar el nivel de riesgo intrínseco, definido como el nivel de impacto ponderado con la probabilidad de ocurrencia de la amenaza.
- Identificar las acciones necesarias (entre estas los controles del Anexo A de la norma ISO 27001) para realizar el tratamiento de los riesgos

evaluados.

- Estimar el riesgo residual luego de los controles tomados.

Niño (2018), menciona que la amenaza es una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando parte de la información y de la TI de la organización. Asimismo, se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza.

Se concluye que un incidente no deseado presenta tres componentes: amenazas, vulnerabilidad e impacto. Las vulnerabilidades indican la debilidad del activo que puede conducir a una amenaza. Si ninguno de estos dos está presente, puede que no se origine un incidente de seguridad ni que surjan riesgos.

I.3.8. Ciclo PHVA

Isotools (2020) y la ISO 9001:2015, describen el ciclo PHVA como:

- Planificar: establecer los objetivos del sistema y sus procesos, y los recursos necesarios para generar y proporcionar resultados previstos de acuerdo con los requisitos del cliente y las políticas de la organización, e identificar y abordar los riesgos y las oportunidades .
- Hacer: implementar lo planificado y medir los resultados obtenidos.
- Verificar: realizar el seguimiento y (cuando sea aplicable) la medición de los procesos y los productos y servicios resultantes respecto a las políticas, los objetivos, los requisitos y las actividades planificadas, e informar sobre los resultados.

- Actuar: tomar acciones para mejorar el desempeño, cuando sea necesario para lograr los resultados deseados.

I.4. Justificación

La presente investigación se centrará en el proceso operativo, el cual es el proceso misional de Core Business Corp., empresa consultora que brinda:

- Provisión de Servicios de Consultoría de Sistemas de Gestión.
- Capacitación (incluido e-learning)
- Auditorías.

Dentro de los activos de información se tienen a los procedimientos de la empresa, la información del clientes, los informes que se le brindan al cliente, los software, hardware, los colaboradores tanto internos como externos, servicios, plataformas digitales, entre otros deben ser protegidos ante robos, perdida, destrucción o manipulación inapropiada.

Debido a que Core Business cuenta con activos de información que al no ser protegidos adecuadamente llevaría a pérdidas económicas, baja reputación a nivel nacional e internacional , perdida de fidelización con los clientes, desconfianza con las partes interesadas y/o perdida y robo de información.

Además, Core Business Corporation SAC en su visión de negocio y la meta de expandirse en el mercado, y llegar a más clientes tiene como uno de sus planes estratégicos implementar un mecanismo que le permita proteger la información, el cual está bajo la normatividad estandarizada ISO 27001:2013 para los procesos operativos de la organización.

Es por ello que la implantación de un SGSI es importante porque permite contar con un Plan de Continuidad del Negocio cuyo objetivo de control es derogar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de

fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna.

Asimismo, en el transcurso de los años las leyes, normativas y requerimientos contractuales van en aumento y se relacionan con la seguridad de la información. Lo genial es que estas se pueden resolver implementando ISO 27001:2013, ya que esta norma proporciona una metodología que ayuda al cumplimiento del ámbito legal.

En relación a lo económico, la filosofía principal de ISO 27001:2013 es evitar que se presenten o sucedan incidentes de seguridad, ya que puede perjudicar a la organización mediante alguna multa, penalidad, o el cierre de un proyecto de alguno de los servicios que brinda.

Esta investigación brinda conocimientos en el ámbito académico, permitiendo conocer el proceso de una implementación relacionada a la ISO 27001:2013. Permitirá que otros alumnos en proceso de desarrollo de una tesis puedan basar su investigación guiándose en la presente tesis, ya que una normativa nueva para muchos, pero con un valor importante, el proteger la información en una organización.

I.5. Perspectiva de términos

Activo de Información: Es todo proceso, tecnología o persona que interviene directa o indirectamente en el procesamiento, transmisión, almacenamiento o destrucción de la información, y por lo tanto tiene valor para la organización. Ej.: instalaciones, hardware, software, personas, soportes de información, servicios, datos e Información, equipamiento auxiliar, etc.

Sistema de Gestión: Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

Mejora continua: es el esfuerzo continuo para mejorar los productos, servicios y procesos mediante pequeñas mejoras incrementales dentro de esas empresas.

Alta dirección: es la persona o conjunto de personas que tienen una responsabilidad general sobre toda la organización, responsables de fijar los objetivos de largo plazo y de definir las estrategias que permita su consecución, resultando ser los responsables del éxito o fracaso de la empresa.

Procesos: Un proceso es una secuencia de acciones que se llevan a cabo para lograr

No conformidad: Incumplimiento de un requisito

Proceso: Conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto.

Confidencialidad: Propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de la información de exactitud y completitud.

Disponibilidad: Propiedad de la información de ser accesible o usable cuando sea demandada por una entidad autorizada.

Riesgo: Efecto que genera incertidumbre sobre el logro de los objetivos de seguridad de información.

I.6. Formulación del problema

¿De qué manera la implementación del Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001:2013 permite proteger la información de los procesos Operativos en la empresa Core Business Corporation SAC ?

I.7. Problemas específicos

- **P1:**¿Cómo se realizará el diagnóstico situacional de la empresa Core Business Corporation SAC?
- **P2:** ¿Cómo se realizará el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013?
- **P3:** ¿ Cómo se elaborará el análisis de riesgo de seguridad de la información?
- **P4:** ¿Cómo se evaluará el desempeño de la seguridad de información de la empresa Core Business Corporation SAC?
- **P5: ¿** Cómo se corroborará la implementación de la ISO 27001:2017 al término de la implementación?

I.8. Objetivos

I.8.1. Objetivo general

Implementar el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para proteger la información en los procesos Operativos en la empresa Core Business.

I.8.2. Objetivos específicos

- **O1:**. Elaborar el diagnóstico situacional de la empresa Core Business Corporation SAC

- **O2:** Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013
- **O3:** Elaborar el análisis de riesgo de seguridad de la información.
- **O4:** Evaluar el desempeño de la seguridad de información de la empresa Core Business Corporation SAC.
- **O5:** Verificar el cumplimiento de la implementación de la ISO 27001:2013.

I.9. Hipótesis

Las hipótesis son las guías de una investigación o estudio, estas indican lo que tratamos de probar y se definen como explicaciones tentativas del fenómeno investigado.(Hernández Sampieri et al., 2014)

Para esta investigación se cuenta con hipótesis general y especificas pertinente a la investigación. Estas hipótesis por utilizar es la descriptiva, para intentar predecir un dato o valor en una o más variables que se van a medir u observar. (Hernández Sampieri et al., 2014)

I.9.1. Hipótesis general

La implementación del Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001:2013 garantiza proteger la información de los procesos operativos de la empresa Core Business.

I.9.2. Hipótesis especificas:

- **H1:** Con el diagnóstico situacional de la empresa se identificará el cumplimiento total de la norma ISO 27001:2013
- **H2:**. Por medio del análisis costo-beneficio se puede determinar la viabilidad económica de la implementación de la ISO 27001:201

- **H3:** Con el análisis de riesgo operacional se garantiza implementar los controles relacionados a la norma ISO 27001:2013.
- **H4:** Evaluar el desempeño de la seguridad de información de la empresa Core Business Corporation SAC. permitirá cumplir con los objetivos de la norma ISO 27001:2013.
- **H5:** Asegurar el cumplimiento de la ISO 27001:2013 permite verificar el desempeño de la implementación.

II. CAPÍTULO. MÉTODO

II.1.Tipo de investigación

II.1.1. Propósito

La presente investigación según su propósito es de tipo aplicado, ya que utiliza las Norma ISO 27001:2015 para resolver la problemática en estudio.

II.1.2. Enfoque

Hernández, Fernández y Baptista (2014) definen que el enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin establecer pautas de comportamiento y probar teorías. (p.4)

El mismo autor define el enfoque cualitativo como el uso de la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación.(p.7)

El presente estudio de investigación tiene el enfoque cuantitativo y cualitativo.

II.1.3. Diseño

La presente investigación es de tipo pre- experimental, el cual consiste en administrar un estímulo o tratamiento a un grupo y después aplicar una medición de una o más variables para observar cuál es el nivel del grupo en éstas, además, no hay manipulación de la variable independiente (niveles) o grupos de contraste (ni siquiera el mínimo de presencia o ausencia). (Hernández, Fernández y Baptista, 2014)

El esquema de este tipo de diseño se muestra a continuación:

G O1 X O2

De acuerdo a lo descrito y visto anteriormente el diseño es pre experimental (con preprueba/posprueba)

Dónde:

G = Grupo de investigación (Proceso operativo de la empresa Corp. Business Corporation)

O1 = Observación (Lista de verificación antes de la implementación)

X = Variable Independiente- Implementación de la ISO 27001:2013(SGSI)

O2= Observación (Lista de verificación luego de la implementación)

II.2.Población y muestra

II.2.1. Población.

La población, viene a ser el conjunto de elementos, sujetos u objetos tomados en cuenta para el desarrollo de la investigación.(Hernández, Fernández & Baptista 2014)

De acuerdo con lo descrito la población para esta investigación es la siguiente:

Para el presente proyecto de investigación, se tomó como población a 6 meses de implementación y certificación que tardaría Core Business Corporation SAC para realizar la implementación de la norma ISO 27001:2013, en el año 2021.

II.2.2. Muestra.

Hernández, Fernández y Baptista (2014), menciona que:

La muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población.

De acuerdo con lo descrito la muestra para esta investigación es la siguiente:

Para el presente proyecto de investigación, se tomó como muestra a 4 meses que conlleva la implementación de la ISO 27001:2013 en Core Business Corporation SAC dentro de los meses de agosto a noviembre considerando los días laborables de lunes a viernes. (97días)

II.3.Técnicas, instrumentos y herramientas de recolección y análisis de datos

II.3.1. Técnicas

Las principales técnicas que utilizaremos en la investigación son: la observación y revisión de documentos.

II.3.1.1. La observación

Como método científico es objetivo, debe entenderse como la correspondencia verdadera entre las observaciones y el objeto observado. (Medina L, et al., 2014)

II.3.1.2. Revisión de documentos

La técnica de revisión de documentos, consiste en la revisión de documentos asociados a la investigación que se pretende efectuar. A menudo, esta revisión documental se realiza con una exploración de documentos de la empresa, luego se realiza la revisión de documentos normativos o de referencias para el trabajo empresarial o se utiliza la teoría científica publicada acerca del tema tratado como las buenas prácticas existentes en el mundo empresarial.(Medina L, et al., 2014)

II.3.2. Instrumentos

Los principales instrumentos que utilizaremos en la investigación son: matriz de consistencia y lista de verificación.

II.3.2.1. Matriz de consistencia

El instrumento es una herramienta metodológica para ordenar, jerarquizar, estructurar y controlar los conceptos, las categorías, las dimensiones y las variables, entre el objeto o fenómeno que se quiere estudiar y los atributos que se le asignan.(Giesecke Sara Lafosse, 2020) (ver anexo 1)

II.3.2.2. Lista de verificación

Los listados de control, listados de chequeo, checklist u hojas de verificación, son formatos realizados para controlar el cumplimiento de un listado de requisitos o recolectar datos ordenadamente y de manera sistemática (ver anexo 2). (Isotools Excelence, s. f.-b)

II.3.3. Herramientas

Las principales herramientas de gestión que utilizaremos en la investigación son: el diagrama de Gantt, matriz de riesgos de SI y la matriz de inventario de activos.

II.3.3.1. Diagrama Gantt

Es una herramienta de gestión que permite planificar y programar actividades a lo largo de un período determinado.(OBS, s. f.)

II.3.3.2. Matriz de riesgos de SI

Es una herramienta de gestión que permite identificar los riesgos más significativos inherentes a las actividades de una organización, tanto de procesos como de fabricación de productos o puesta en marcha de servicios. (Isotools Excelence, s. f.-a)

Tabla 3

Técnicas, instrumentos y herramientas de recolección y análisis de datos

Etapa	Técnica	Descripción	Instrumento	Herramienta
Recolección de datos	Observación	Es objetivo, debe entenderse como la correspondencia verdadera entre las observaciones y el objeto observado. Además, el problema de la objetividad alcanza tanto la validez de los resultados obtenidos como su generalización. (Medina L, et al., 2014)	matriz de consistencia, Lista de verificación (Check List de cumplimiento de las cláusulas)	FODA Diagrama Gantt
Análisis de la situación problemática	Revisión de documentos.	Consiste en la revisión de documentos asociados a la investigación que se pretende efectuar. Esta revisión documental se realiza con una exploración de documentos de la empresa, luego se realiza la revisión de documentos normativos o de referencias para el trabajo empresarial o se utiliza la teoría científica. (Medina L, et al., 2014)	Lista de verificación(Check List de cumplimiento de las cláusulas)	Diagrama Gantt Matriz de inventario de activos Matriz de riesgos de SI

Nota. En el cuadro siguiente de resumen las técnicas e instrumentos a usar en la presente investigación.

II.4. Procedimiento

Para la realización de la implementación se tomará en cuenta la estructura de la ISO 27001:2013, la cual se muestra en la tabla 4.

Tabla 4

Procedimiento

Objetivo	Etapa	Descripción
O1: Elaborar el diagnóstico situacional de la empresa Core Business Corporation SAC		Se realizará la lista de verificación (check list) para verificar el cumplimiento de la ISO 27001:2013, tomando en cuenta los requisitos de la propia norma.
O2: Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013.		Se tomará en cuenta el costo antes de la implementación de la norma ISO 27001:2013.
O3: Elaborar el análisis de riesgo de seguridad de la información.	Planear (Establecer el SGSI)	Se tomará en cuenta los requisitos siguientes: 4.Contexto: ● Entendimiento de la organización y su contexto. ● Las expectativas de las partes interesadas. ● El alcance del SGSI. 5.Liderazgo: ● Liderazgo y compromiso de la alta dirección. ● Políticas ● Roles, responsabilidades y autoridades. 6.Planeación: ● Riesgos y oportunidades. 7. Soporte: ● Recursos, Competencia, Conciencia, Comunicación y Conciencia.

Se utilizo el ciclo PHVA teniendo en cuenta con los requisitos de la ISO 27001:2013

Tabla 4

Procedimiento

Objetivo	Etapa	Descripción
O3: Elaborar el análisis de riesgo de seguridad de la información.	Hacer (Implementar y operar el SGSI)	Se tomará en cuenta el requisito: 8. Operación: ● Planificación y control operacional ● Evaluación de riesgos de SI ● Tratamiento de riesgos de la SI Se implementará la política, los controles, procesos y procedimientos del SGSI de acuerdo a los controles que se tomaran.
O4: Evaluar el desempeño de la seguridad de información de Core Business Corporation SAC.	Verificar (Monitorear y revisar el SGSI)	Se tomará en cuenta el requisito: 9.Evaluación del desempeño ● Seguimiento, medición, análisis y evaluación ● Auditoria internas ● Revisión por la dirección Evaluar, y donde sea aplicable, medir el rendimiento del proceso de la política del SGSI, sus objetivos, e informar los resultados para gestionar su revisión.
O4: Evaluar el desempeño de la seguridad de información de Core Business Corporation SAC.	Actuar (Mantener y mejorar el SGSI)	Se tomará en cuenta el siguiente requisito: 10.Mejora ● No conformidad y acciones correctivas ● Mejora continua Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI
O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013.		Se realizará la lista de verificación (check list) al término de la implementación, para verificar el

	cumplimiento de la ISO 27001:2013, tomando en cuenta los requisitos de la propia norma.
Se utilizo el ciclo PHVA teniendo en cuenta con los requisitos de la ISO 27001:2013	

II.4.1. Diagrama Gantt

Para dar inicio al procedimiento se contará con el diagrama Gantt para dar seguimiento a las principales actividades a realizar para el proyecto de implementación del sistema de gestión de seguridad de la información. (Ver anexo 3)

II.5. Método de análisis de datos

Hernández (2010), menciona que los métodos de análisis de datos se definen:

"Al analizar los datos cuantitativos debemos recordar dos cuestiones: primero, que los modelos estadísticos son representaciones de la realidad, no la realidad misma; y segundo, los resultados numéricos siempre se interpretan en contexto" (p.270).

Para la presente investigación utilizaremos el método de análisis descriptivo, se tabulará la información en tablas y frecuencia calculando sus porcentajes e incidencias, incluso su rango según sea el caso, representando la información en gráficos.

Rustom (2012), sostiene que la estadística descriptiva es "válido para el conjunto de datos descrito y se realiza mediante: tablas de frecuencias y/o porcentajes, gráficos, medidas […], además de hacer inferencias" (p.11).

Por otro lado, los aspectos teóricos han sido adquiridos estrictamente respetando los derechos de autor los cuales han sido citados en cada uno de los conceptos utilizados, además de ello se ha tomado las evidencias de acuerdo con lo observado sin manipulación de estas.

II.5.1. Validez

Behar (2008) detalló que la validez "indica la capacidad de la escala para medir las cualidades para las cuales ha sido construida y no otras parecidas" (p.73).

En el presente trabajo de investigación se considerará el juicio de expertos (ver anexo 4) que cuenten con el grado académico requerido para la validación, teniendo la tarea de validar el uso del instrumento (lista de verificación).

Los 3 expertos fueron los siguientes:

- Ing. Dante Velásquez Aliaga
- Ing. Paul Aliaga Mori
- Ing. Abby cruz Rodríguez

II.5.2. Confiabilidad

Behar (2008) detalló que: "se refiere a la consistencia interior de la misma, a su capacidad para discriminar en forma constante entre un valor y otro" (p.73).

II.6. Aspectos Éticos

Los aspectos éticos que se consideran en esta investigación son el consentimiento informado y confidencialidad. El primero de ellos se consideró ya que los informantes estuvieron de acuerdo en ser parte de la investigación reconociendo sus derechos y deberes durante el estudio. El segundo porque se actuó con ética durante el desarrollo de la investigación y se asumió responsabilidad de los resultados obtenidos durante la recolección de datos.

III. CAPÍTULO. RESULTADOS

III.1. Objetivo 1. Elaborar el diagnóstico de la empresa.

Con el objetivo de medir el nivel actual de cumplimiento de la ISO 27001:2013 en los procesos Operativos de la empresa Corp. Business Corporation SAC se utilizó la lista de verificación que cuenta con los requisitos de la norma ISO 27001:2013. (ver anexo 2)

Contando esta con el siguiente criterio de calificación:

Tabla 5

Calificación del Check list

Calificación	SIGNIFICADO
[0% ; 25%>	No han identificado ni desarrollado actividad alguna para cumplir este requisito o no se dispone de evidencias
[25% ; 50%>	Han identificado actividades para cumplir este requisito y se encuentran en desarrollo
[50% ; 75%>	Las actividades han sido identificadas y desarrolladas, pero no se ajustan plenamente a la norma o están implementadas parcialmente
[75% ; 100%>	Las actividades han sido implementadas y se ajustan al estándar considerado como criterio de evaluación (actividades aprobadas e implementadas)
100%	Además de lo anterior las actividades han sido validadas y muestran mejoras

Para realizar el check list se tomó la calificación mencionada para dar un porcentaje al cumplimiento de la ISO 27001:2013

Concluyendo con ello, que Core Business Corp. SAC cuenta con el 39% de cumplimiento. (Ver tabla 6)

Tabla 6

Cumplimiento de la norma ISO 27001:2013 antes de la implementación

CAPITULO	% POR CAPITULO	SIGNIFICADO
4	**75%**	Las actividades han sido implementadas y se ajustan al estándar considerado como criterio de evaluación (actividades aprobadas e implementadas)
5	**42%**	Han identificado actividades para cumplir este requisito y se encuentran en desarrollo
6	**0%**	No han identificado ni desarrollado actividad alguna para cumplir este requisito o no se dispone de evidencias
7	**29%**	Han identificado actividades para cumplir este requisito y se encuentran en desarrollo
8	**17%**	No han identificado ni desarrollado actividad alguna para cumplir este requisito o no se dispone de evidencias
9	**58%**	Las actividades han sido identificadas y desarrolladas, pero no se ajustan plenamente a la norma o están implementadas parcialmente
10	**50%**	Las actividades han sido identificadas y desarrolladas, pero no se ajustan plenamente a la norma o están implementadas parcialmente
TOTAL	39%	

Mediante el check list se observa el cumplimiento de la norma ISO 27001:2013 contando con un promedio del 39% de cumplimiento.

En los siguientes párrafos se detalla los requisitos de la norma dando respuesta a los objetivos planteados, además de identificar formatos y procedimientos que se evidencian en la lista maestra(ver anexo 5), la cual se actualizo, para la implementación de SGSI.

III.2. Objetivo 2. Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013.

Para el desarrollo de implementación se analizó el costo/beneficio para conocer la viabilidad del proyecto.

Para la presente investigación, se tomará en cuenta los costos y beneficios de la implementación de manera semestral que asumirá Core business Corporation. La implementación cuenta con un tiempo de 4 meses y con ello da lugar a que en los 2 meses siguientes se realicen las auditorías internas y externas para lograr así continuar con una certificación, además estos costos pueden incrementaran debido a los posibles controles que la propia organización requiera, como sistemas informáticos, costo de antivirus, software especializado para control de accesos, herramientas de encriptaciones pero estos no son tomados en esta etapa de implementación, ya que la organización cuenta con algunos de ellos mas no están siendo gestionadas adecuadamente.

Po un lado, contamos con costos en RRHH, de implementación ,y formación y capacitación los cuales se mencionarán en las siguientes tablas: (ver tabla 7 y 8)

Tabla 7

Costos de RRHH

Tipo	Descripción	Tarifa por horas	cantidad de horas	Costo Total
Costo de RRHH	Responsable de desarrollo de procesos	S/ 4.38	320	S/ 1,400.00
Costo de RRHH	Analista Junior de Business Inteligencie	S/ 4.38	320	S/ 1,400.00
Costo de RRHH	Oficial de seguridad	S/ 20.83	320	S/ 6,666.67
Total				**S/ 9,466.67**

Tabla 8

Costo Total según su tipo

Tipo	Descripción	Costo Total
Costo de Formación o Capacitación	Capacitación de ISO 27001:2013	S/ 1,500.00
Costo de Formación o Capacitación	Asesorías en ISO 27001:2013	S/ 1,550.00
Costo de implementación	Auditoría Interna	S/ 3,500.00
Costo de implementación	Auditoría Externa	S/ 3,500.00
Costo de implementación	Certificación 27001:2013	S/ 7,000.00
Costos tecnológicos	Licencias de antivirus (McAfee, Avast)	S/ 131
Costos tecnológicos	Licencia de Office	S/ 288.00
Costo RRHH	Oficial de SI/Responsable de procesos /Analista Junior de Business Inteligencie	S/ 9,466.67
COTO TOTAL		**S/ 26,935.92**

El costo total que conlleva al logro de implementación y por ende la certificación es de **S/ 26,935.92 .**

En cuanto al beneficio, se enfoca a la reducción de los riesgos de seguridad de la información, así como reducción de futuras amenazas o vulnerabilidades de los activos de información, capacidad de transferir riesgos de manera selectiva, lo cual conllevara ha ahorros de costos. Además, los beneficios de la certificación ISO 27001:2013, promueven la imagen de Core Business como un socio seguro para los negocios teniendo así una ventaja competitiva, garantizando a sus partes interesadas el compromiso de la organización en seguridad de la información.

Por ello, Core Business Corporation cuenta con el beneficio de ahorro que asume en pérdidas económicas relacionadas a los incidentes de seguridad de la información,

disminuyendo así los reclamos por parte de sus clientes, ya que al contar con los controles establecidos por la norma ISO 27001:2013 no se tendría que asumir el pago por multas de acuerdos con los clientes, perdida de un proyecto y/o hardware el cual fue establecida por el socio principal de la organización.(ver tabla 8)

Tabla 9

Beneficio

Ahorro de implementación del SGSI	Beneficio
perdida de laptop	S/ 2,500.00
perdida de disco duro	S/ 350.00
perdida de USB	S/ 50.00
Crear, modificar, divulgar información del cliente(penalidades por parte del cliente)	S/ 50,000.00
AHORRO TOTAL	**S/ 52,900.00**

El beneficio total que conlleva al logro de implementación y por ende la certificación es de **S/ 52,900.00**

De acuerdo a ello, el costo/beneficio es el siguiente:

Tabla 10

Costo/beneficio

costo	S/ 26,935.92
beneficio	S/ 52,900.00
Beneficio/Costo	**1.96**

Debido a que el beneficio resulto mayor a 1, el proyecto es rentable para Core Business Corporation, ya que por cada sol invertido se gana 1.96 soles.

III.3. Objetivo 3. Elaborar el análisis de riesgo de seguridad de la información

III.3.1. Planear

Dentro de esta etapa planear se hará uso de los requisitos 4 al 7 de la normativa ISO 27001:2013.

III.3.1.1. Contexto de la organización

III.3.1.1.1. Comprender la organización y su contexto

Core Business Corp. SAC es una empresa con más de 7 años en experiencia, brinda soluciones de alto valor para la mejora del Core Business de sus socios estratégicos, que los ayuden a posicionar su liderazgo en cada uno de sus sectores. La comprensión de las necesidades del entorno, la innovación de nuestros procesos y el compromiso de nuestros profesionales ayudan a generar seguridad y confianza a las partes interesadas, en especial a nuestros clientes. Los servicios están enfocados en la seguridad y salud del trabajador, gestión de calidad, prevención de casos de corrupción, soborno y rediseño organizacional, están liderados por las 3 líneas de negocios:

- Sistemas de Gestión
- Desarrollo Organizacional
- Formación y Capacitación

Cada una cumple los parámetros de medición y análisis definidos por entidades competentes y recomendadas a escala mundial como la NIOSH, OSHA, COSO, ISO e INACAL, con el fin de asegurar a nuestros clientes resultados confiables y efectivos.

III.3.1.1.1.1. Misión

Asesorar y facilitar a los grupos de interés con el personal competente y la aplicación de la última tecnología; para el desarrollo, implementación y mantenimiento de sus Sistemas de Gestión, brindado un alto valor al negocio de la organización.

III.3.1.1.1.2. Visión

Para el 2023, ser reconocida entre las 05 mejores firmas consultoras de Sistema de Gestión en el Perú, a base de soluciones de alto valor y contribuyendo al cumplimiento de los objetivos de nuestros socios estratégicos.

III.3.1.1.1.3. Foda

Se analiza el contexto de la organización mediante un FODA, el cual se evalúa mediante los factores tecnológico, social, recursos humanos, operaciones. (ver figura 6)

Figura 5

Foda

ORIGEN	FACTOR A EVALUAR	CODIGO	OPORTUNIDADES	Sistema de Gestión	IMPACTO BSC	ÁREAS RELACIONADAS
EXTERNO	TECNOLOGICO	O1	Avances de la tecnología para la implementación de Sistemas de Gestión	SIG	Procesos	Desarrollo de Procesos, Gestión de Proyectos
	COMPETITIVO	O2	La competencia NO se ha posicionado	SGC	Clientes	Administración y Finanzas
	SOCIAL	O3	Mayor oferta de Entidades especializadas para la formación.	SIG	Capital Humano	Administración y Finanzas
	SOCIAL	O4	COVID19 (Enfoque de necesidad por parte del cliente)	SGC	Clientes	Todas
	POLITICO	O6	Regulaciones en beneficios de los Sistemas de Gestión	SIG	Procesos	Gestión de Proyectos
	SOCIAL	O7	Fiscalización de la SUNAFIL: Potenciales demandas laborales frente a incumplimientos (Enfoque cliente)	SIG	Clientes	Gestión de Proyectos
	SOCIAL	O8	Poca normativa técnica nacional que regule el tema de seguridad. (Riesgos críticos)	SIG	Procesos	Gestión de Proyectos
	FACTOR A EVALUAR	**CODIGO**	**AMENAZAS**	**Sistema de Gestión**	**IMPACTO BSC**	**ÁREAS RELACIONADAS**
	COMPETITIVO	A1	Nuevos competidores extranjeros	SGC	Accionistas	Gestión de Proyectos
	POLITICO	A2	Regulación para consultores	SGC	Capital Humano	Administración y Finanzas
	COMPETITIVO	A3	Crecimiento de empresas consultorias: estrategia comercial agresiva	SGC	Clientes	Todas
	ECONOMICO	A4	Estancamiento de la Economía (Consultoría). Potenciales proyectos.	SGC	Accionistas	Administración y Finanzas
	SOCIAL	A5	COVID19 (contagio a nuestros colaboradores)	SST	Capital Humano	Desarrollo de Procesos, Administración y Finanzas
	TECNOLOGICO	A6	Ataques cibernéticos, robos, perdidas de información	SIG	Clientes	Administración y Finanzas
ORIGEN	**FACTOR A EVALUAR**	**CÓDIGO**	**FORTALEZAS**	**Sistema de Gestión**	**IMPACTO BSC**	**ÁREAS RELACIONADAS**
INTERNOS	RECURSOS HUMANOS	F1	Buena valoración como lugar de trabajo, flexibilidad para el teletrabajo	SIG	Capital Humano	Todas
	OPERACIONES	F2	Empresa en enfoque al servicio al cliente (Filosofia).	SGC	Clientes	Desarrollo de Procesos, Gestión de Proyectos
	RECURSOS HUMANOS	F3	Conocimiento del Mercado: 7 años. (Comparación con la competencia)	SGC	Capital Humano	Administración y Finanzas
	RECURSOS HUMANOS	F4	Know How técnico, Profesionalismo en Sistemas de Gestión	SIG	Capital Humano	Gestión de Proyectos
	FACTOR A EVALUAR	**CÓDIGO**	**DEBILIDADES**	**Sistema de Gestión**	**IMPACTO BSC**	**ÁREAS RELACIONADAS**
	RECURSOS HUMANOS	D1	Conocimientos en riesgos especializados	SGC	Capital Humano	Administración y Finanzas
	OPERACIONES	D2	No contamos con la capacidad de brindar el soporte integral de SST (Higiene, Ergonomía, Salud, Psicología)	SGC	Capital Humano	Administración y Finanzas
	SISTEMAS DE INFORMACIÓN	D3	Plataforma tecnológica para la gestión de la empresas.	SIG	Procesos	Administración y Finanzas
	OPERACIONES	D4	Procesos no consolidados: Demoras en los tiempos de entregables	SGC	Procesos	Desarrollo de Procesos, Gestión de Proyectos
	MARKETING	D5	Nuestro posicionamiento solo es SST.	SGC	Clientes	Administración y Finanzas

III.3.1.1.2. Comprender las necesidades y expectativas de las partes interesadas

Se determinan quiénes son las partes interesadas y los requisitos que sean pertinentes a la seguridad de la información.

Tabla 11

Partes interesadas y requisitos

PARTES INTERESADAS	REQUISITOS
Estado (SUNAT)	Cumplimiento de obligaciones tributarias
Estado (SUNAFIL, Ministerio del Trabajo, Ministerio de Salud, INDECOPI, MINJUS,ANPD) y otras entidades	Cumplimiento de normas laborales y legales para el cuidado de los trabajadores en temas de seguridad de información.
Estado (INACAL)	Cumplimiento de las normas técnicas para brindar la consultoría
Accionistas	Lineamientos de la empresa Pago de Remuneraciones Beneficios Laborales Evaluación de Desempeño
Colaboradores	Cumplimiento de las normativas relacionadas(Ley de Protección de Datos Personales – 29733, ley sobre el Derecho de Autor - DL 822 y la ley de Delitos Informáticos – 30096)
Cliente	Cumplimiento de los requisitos contractuales. Cumplimiento de los lineamientos de la empresa Cumplimiento de acuerdos y/o contratos (confidencialidad y seguridad)
Proveedores	Pago de remuneraciones/evaluación de Proveedores/ lineamientos de la empresa.

Fuente: Core Business Corporation SAC

III.3.1.1.3. Determinar el alcance del sistema de gestión

Por ser una organización pequeña, y debido a que la información involucra a todas las áreas el alcance del sistema de gestión es el siguiente:

"Core Business Corporation, establece, implementa, opera, verifica y mejora el SGSI cubriendo toda la información que queda expuesta a sufrir cambios, alteraciones o robo de los activos de información al proceso principal el cual es el operativo."

Además, se debe tener en cuenta que Core Business Corp. SAC labora bajo la modalidad de trabajo remoto.

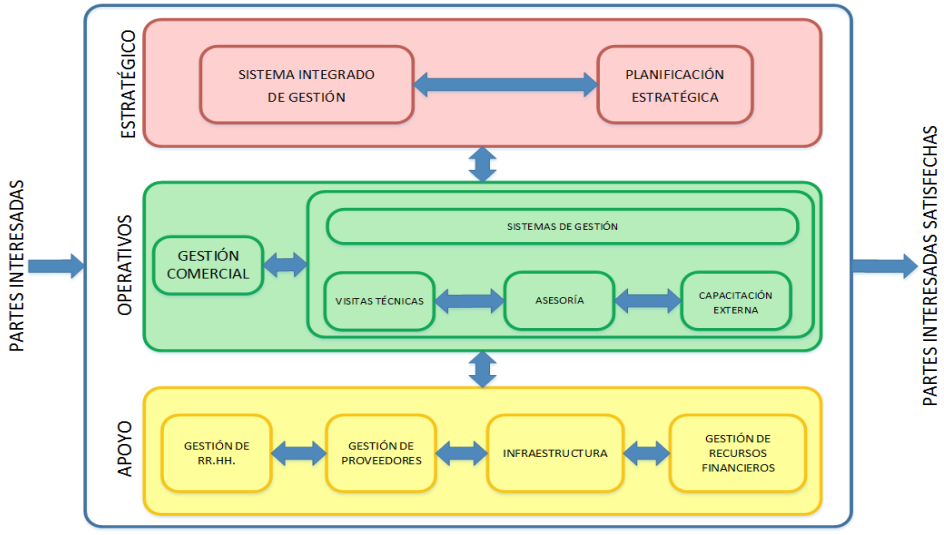
Asimismo, se determina los límites y aplicabilidad de los controles del sistema de gestión de seguridad de la información en el FOR.064 Aplicabilidad.(Ver anexo 6)

III.3.1.1.4. Sistema de gestión de seguridad de la información

Core Business Corporation SAC (CBC) establece, implementa, mantiene y mejora continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma ISO 27001:2013. (Ver figura 7)

Figura 6

Mapa de proceso



Fuente: Core Business Corp. SAC.

III.3.1.2. Liderazgo

III.3.1.2.1. Liderazgo y compromiso

La alta dirección de CBC está integrada por el Socio Principal y Business Partner, los cuales demuestran liderazgo y compromiso:

a) Asegurándose de que se establezcan la POL.001 Política de Excelencia Organizacional (ver figura 8) y los FOR.002 Objetivos e indicadores (ver anexo 7), y que éstos sean compatibles con el contexto y la dirección estratégica de la organización.

b) Asegurándose de la integración de los requisitos del sistema de gestión de SI en los procesos de negocio de la organización; mediante el FOR.001 Mapa de Procesos (ver figura 7) y POL.008. Caracterización de procesos. (ver anexo 8)

c) Asegurándose de que los recursos necesarios para el sistema de gestión SI estén disponibles, mediante el FOR.003 Programa anual del Sistema de Gestión (ver anexo 9) y la POL.008. Caracterización de procesos.

d) Comunicando la importancia de un sistema de gestión SI eficaz y conforme con los requisitos del sistema de gestión; mediante el FOR.033. Programa anual de comunicación y sensibilización.

e) Asegurándose de que el sistema de gestión SI logre los resultados previstos; mediante el seguimiento y cumplimiento de los FOR.002 Objetivos e indicadores.

f) Comprometiendo, dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión, mediante el FOR.016. Programa anual de capacitación(ver figura 14), FOR.033. Programa anual de comunicación y sensibilización (ver figura 15) y la ejecución de las reuniones de Comités internos plasmadas en el FOR.004 Acta de Comité (ver anexo 10).

g) Mediante reuniones o comités internos (FOR.004), se apoya a otros roles pertinentes de la dirección, con el fin de demostrar su liderazgo. Áreas de responsabilidad.

- Jefe de Administración y Finanzas
- Responsable de Desarrollo de Procesos.
- Consultor Líder

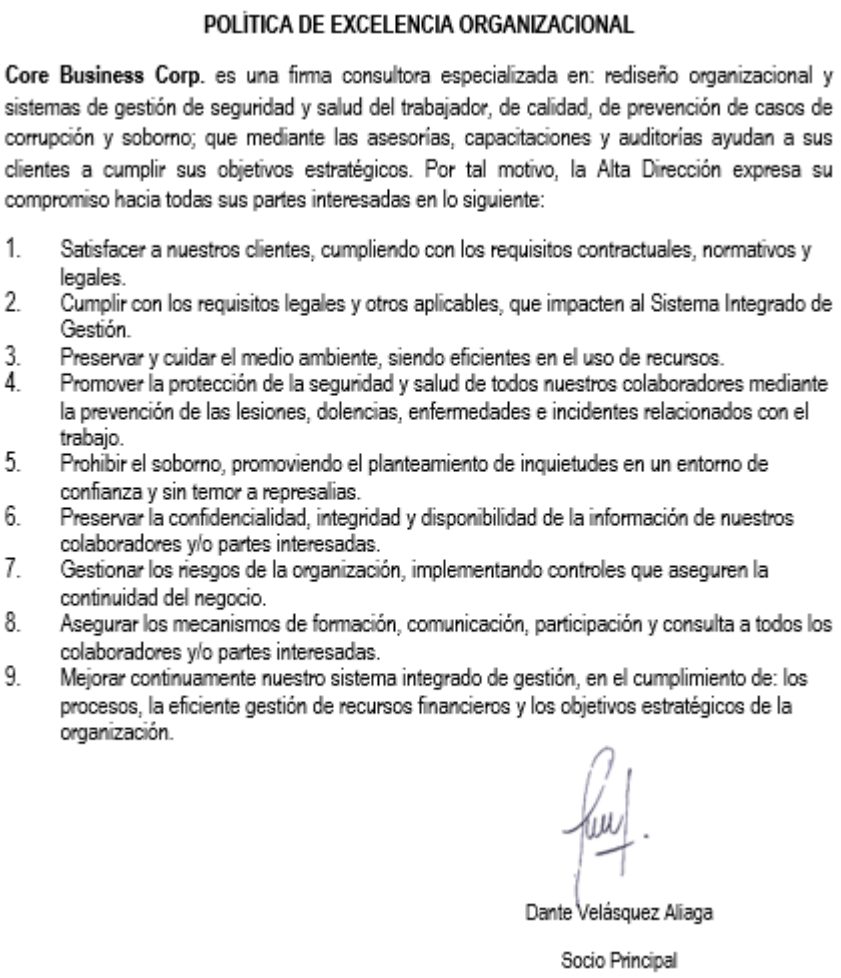
h) Promoviendo la mejora; mediante la política POL.001 Política de Excelencia Organizacional.

III.3.1.2.2. Política

La política de excelencia organizacional de CBC está definida en el documento POL.001 Política de Excelencia Organizacional. En el cual se evidencia la política N° 6 enfocada a la seguridad de la información. (ver figura 8)

Figura 7

Política de excelencia organizacional



POLÍTICA DE EXCELENCIA ORGANIZACIONAL

Core Business Corp. es una firma consultora especializada en: rediseño organizacional y sistemas de gestión de seguridad y salud del trabajador, de calidad, de prevención de casos de corrupción y soborno; que mediante las asesorías, capacitaciones y auditorías ayudan a sus clientes a cumplir sus objetivos estratégicos. Por tal motivo, la Alta Dirección expresa su compromiso hacia todas sus partes interesadas en lo siguiente:

1. Satisfacer a nuestros clientes, cumpliendo con los requisitos contractuales, normativos y legales.
2. Cumplir con los requisitos legales y otros aplicables, que impacten al Sistema Integrado de Gestión.
3. Preservar y cuidar el medio ambiente, siendo eficientes en el uso de recursos.
4. Promover la protección de la seguridad y salud de todos nuestros colaboradores mediante la prevención de las lesiones, dolencias, enfermedades e incidentes relacionados con el trabajo.
5. Prohibir el soborno, promoviendo el planteamiento de inquietudes en un entorno de confianza y sin temor a represalias.
6. Preservar la confidencialidad, integridad y disponibilidad de la información de nuestros colaboradores y/o partes interesadas.
7. Gestionar los riesgos de la organización, implementando controles que aseguren la continuidad del negocio.
8. Asegurar los mecanismos de formación, comunicación, participación y consulta a todos los colaboradores y/o partes interesadas.
9. Mejorar continuamente nuestro sistema integrado de gestión, en el cumplimiento de: los procesos, la eficiente gestión de recursos financieros y los objetivos estratégicos de la organización.

Dante Velásquez Aliaga

Socio Principal

Además, se establecieron las Políticas de seguridad de la información (ver anexo 11):

- POL.011 Política Dispositivos móviles
- POL.012 Política Trabajo remoto
- POL.013 Política Control de acceso
- POL.014 Política Escritorio limpio y pantalla limpia
- POL.015 Política de proveedores

La política esta:

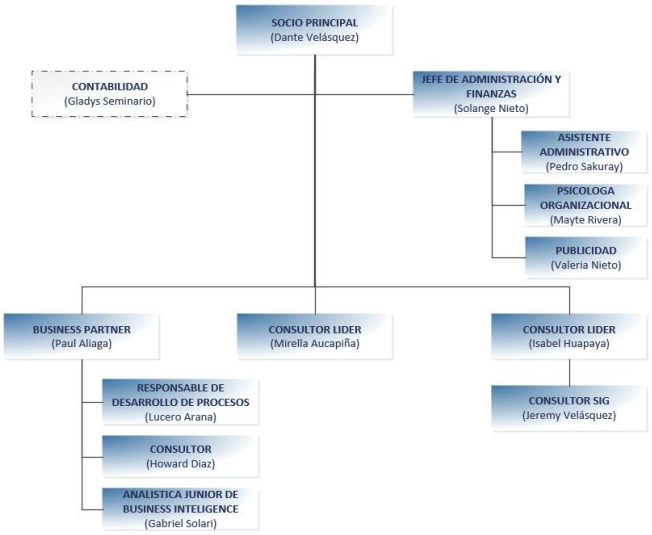
- Disponible y se mantiene como información documentada; por medio del repositorio de SharePoint de CBC, en la página web, correo.
- Comunicarse, entenderse y aplicarse dentro de la organización; por medio del FOR.033. Programa de comunicaciones y sensibilización.
- Estar disponible para las partes interesadas pertinentes, por medio de la Web, envío de correo electrónico y reuniones con proveedores.

III.3.1.2.3. Roles, responsabilidades y autoridades organizacionales

La alta dirección se asegura que las responsabilidades y autoridades para los roles pertinentes se asignen, mediante el MAN.001 Manual de Organización y Funciones (ver anexo 12), POL.009 Rendición de Cuentas(ver anexo 13) y FOR.010. Organigrama (ver figura 12) se comuniquen y se entiendan, mediante los Comités internos y envío de documentación.

Figura 8

Organigrama



Fuente: Core Business Corporation SAC

La alta dirección asigna la responsabilidad y autoridad al responsable de Desarrollo de Procesos, para:

a) Asegurar que el sistema de seguridad de la información es conforme con los requisitos de las normas ISO 27001, mediante la aplicación del FOR.003 Programa anual y el POL.003 Alcance.(ver anexo 14)
b) Informar a la alta dirección sobre el desempeño del sistema Integrado de gestión y sobre las oportunidades de mejora, mediante la Revisión por la Dirección.

Por ello, se cuenta con las siguientes responsabilidades que están ligadas a la seguridad de información:

- Oficial de Seguridad de la Información

1. Informar al Socio principal sobre el desempeño del SGSI.
2. Organiza la realización de las auditorías internas y externas del SGSI.
3. Promueve la capacitación y concientización de los colaboradores acerca de la gestión de la seguridad de la información.
4. Lidera los proyectos de mejora del SGSI.

- Propietario del Activo de Información

1. Controla el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le corresponde.
2. Autorizar el uso del activo de información del cual es propietario, bajo su responsabilidad, de esta manera se preserve la seguridad de la información.

3. Entender y abordar los riesgos relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
4. Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

❖ Usuario del Activo de Información

1. Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le corresponde.
2. Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.

❖ Propietario del Riesgo

Asegurar que se implementen los controles de seguridad definidos para reducir a un nivel aceptable el riesgo que le fue asignado.

III.3.1.3. Planificación

III.3.1.3.1. Acciones para tratar los riesgos y las oportunidades

III.3.1.3.1.1. Generalidades

Al planificar el sistema, CBC considera el análisis de las cuestiones externas e internas definidas y partes interesadas en el FOR.015 - Análisis de Contexto y Partes interesadas (Ver figura 9), además determina los riesgos y oportunidades, definidos en el PRO.005. Procedimiento de gestión de riesgos y oportunidades (ver anexo 15), los cuales:

a) Aseguran que el SGSI logre sus resultados previstos.
b) Aumenten los efectos deseables.
c) Reduzcan los efectos no deseados.

d) Logren la mejora.

e) CBC Planifica:

- Las acciones para abordar estos riesgos y oportunidades; los cuales son proporcionales al impacto potencial en la conformidad de los servicios.
- La integración e implementación de las acciones en sus procesos del SGI
- La evaluación de la eficacia de estas acciones.

III.3.1.3.1.2. Valoración del riesgo de seguridad de la información

Se elaboro el procedimiento PRO.025 Gestión de activos (ver anexo 16), procedimiento de gestión de riesgos operacionales de seguridad de la información(ver anexo 17) y el formato FOR.062 Inventario de activos (ver tabla 9) para documentar el desarrollo del proceso.

El responsable de desarrollo de procesos juntamente con el Business Partner y el socio principal registran los activos de información en el FOR.062 Formato de inventario de activos, cuenta con los siguientes criterios: Categoría del activo, Nombre del activo, Descripción, Proceso, Subproceso, Propietario, custodio y usuario, Ubicación (física y digital). (ver tabla 8).

III.3.1.3.1.2.1. Valorización de activos de información

El Socio principal y Business Partner realizan la valoración de un los activos de Información.

Esta dependerá de la pérdida económica de acuerdo a la siguiente tabla:

Tabla 12

Valoración de activo

NIVEL	RANGO(DINERO)		DESCRIPCIÓN
1	0	3000	La pérdida económica es baja.
2	3000	10000	La pérdida económica es moderada.
3	10000	25000	La pérdida económica es relevante.
4	25000	50000	La pérdida económica es alta
5	50000	+	La pérdida económica es critica

Para realizar la valoración del activo se realizó una reunión con la alta dirección, tomándose en cuenta la pérdida económica que afectaría el no tener el activo.

Tabla 13

Inventario de Activos

FORMATO Código: FOR.062

INVENTARIO DE ACTIVO Fecha: 21/09/2021 VERSIÓN: 01

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Datos/Información	ESTRATEGICO	SIG	A1	Procedimiento del SIG	Todos los procedimientos de la ISO 9001:2015	Responsable de desarrollo SIG	Todos los colaboradores	No aplica	USO INTERNO	MS SharePoint Online/SIGCBC	1	BAJO
Datos/Información	OPERATIVO	Gestión Comercial	A2	Información del cliente	Información de inspecciones, auditorias, visitas técnicas y asesorías que brinda la empresa.	Socio Principal	Consultores Lideres	No aplica	CONFIDENCIAL	MS SharePoint Online Drive	5	ALTO
Datos/Información	OPERATIVO	Gestión Comercial	A3	Informes de proyectos	ejecución y evaluación de los servicios de inspecciones, auditorias, visitas técnicas y asesorías que brinda la empresa.	Consultores Lideres	Clientes	No aplica	CONFIDENCIAL	Drive	4	ALTO
Datos/Información	APOYO	Gestión de Recursos Financieros	A4	Contratos	Acuerdo escrito, por el que CBC y partes interesadas se comprometen recíprocamente a respetar y cumplir una serie de condiciones.	Jefa de administración y finanzas	Colaboradores Proveedores Clientes	No aplica	CONFIDENCIAL	MS SharePoint Online(Grupo Gestión Humana)	2	MEDIO

Tabla 14

Inventario de Activos

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Datos/Información	APOYO	Infraestructura	A5	Copias de respaldo de Información de CBC	Información de CBC	Socio Principal	Socio Principal	Discos duros	CONFIDENCIAL	No aplica	4	ALTO
Datos/Información	APOYO	Infraestructura	A6	Copias de respaldo de Información a nivel de usuario	información de usuario	Socio Principal	Socio Principal	Discos duros	CONFIDENCIAL	No aplica	4	ALTO
Datos/Información	APOYO	Gestión de Recursos Financieros	A7	Mensajería(Correo corporativo)	Información, comunicación brindada a clientes, colaboradores, entre otros.	Jefa de administración y finanzas	Jefa de administración y finanzas Business Partner	No aplica	USO INTERNO	Outlook	2	MEDIO
Servicios	APOYO	Infraestructura	A8	MS SharePoint Online	Aplicativo de gestión documental	Responsable de desarrollo SIG	Todos los colaboradores(Personal Interno)	No aplica	No aplica	Servidor de aplicación virtual/Microsoft	5	ALTO
Servicios	APOYO	Infraestructura	A9	Google drive	Alojamiento de archivos	Consultores Líder	Todos los colaboradores	No aplica	No aplica	Google Drive	4	ALTO

Tabla 15

Inventario de Activos

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Servicios	APOYO	Infraestructura	A10	E-learning-Intranet	Almacenamiento de la información con contenido web para uso interno de CBC	Business Partner	Personal Interno	No aplica	No aplica	Página Web	2	MEDIO
Servicios	APOYO	Infraestructura	A11	Página Web	Almacenamiento de la información con contenido web	Business Partner	Público en general	No aplica	No aplica	Servidor virtual(proveedor)	2	MEDIO
Servicios	APOYO	Infraestructura	A12	Outlook	correo electrónico Corporativo	Jefe de administrador y finanzas	Todos los colaboradores	No aplica	No aplica	servidor de aplicación virtual Microsoft	3	MEDIO
Servicios	APOYO	Infraestructura	A13	Poder Apps	Proporciona un entorno de desarrollo de aplicaciones ágil para crear aplicaciones personalizadas para las necesidades de CBC	Consultores Lideres Analista de Power BI	Todos los colaboradores (Uso interno)	No aplica	No aplica	Power Mate	2	MEDIO
Servicios	APOYO	Infraestructura	A14	LinkedIn	Redes sociales	Comunicaciones(Valeria)	Todos los colaboradores y Externos	No aplica	No aplica	Servidor virtual(proveedor)	1	BAJO
Servicios	APOYO	Infraestructura	A15	Facebook	Redes sociales	Comunicaciones(Valeria)	Todos los colaboradores y Externos	No aplica	No aplica	Servidor virtual(proveedor)	1	BAJO

Tabla 16

Inventario de Activos

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Software	APOYO	Infraestructura	A16	Adobe/Acroba	Software Microinformático	Responsable Soporte técnico	Todos los colaboradores	No aplica	No aplica	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	1	BAJO
Software	APOYO	Infraestructura	A17	Herramientas de Office	Software Microinformático	Responsable Soporte técnico	Todos los colaboradores	No aplica	No aplica	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	1	BAJO
Software	APOYO	Infraestructura	A18	Microsoft Windows(Sistema Operativo)	Software que permite la administración del hardware de los equipos de cómputo (Escritorio, portátiles, servidores)	Responsable Soporte técnico	Todos los colaboradores	No aplica	No aplica	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	3	MEDIO
Software	APOYO	Infraestructura	A19	Antivirus	Software orientado a proteger la red de código malicioso (Malware)	Responsable Soporte técnico	Todos los colaboradores	No aplica	No aplica	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	4	ALTO
Software	APOYO	Infraestructura	A20	AutoCAD	software de diseño asistido por computadora (CAD)	Responsable Soporte técnico	Colaboradores definidos(Isabel, Comunicación)	No aplica	No aplica	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	1	BAJO

Tabla 17

Inventario de Activos

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Hardware (Equipamiento Informático)	APOYO	Infraestructura	A21	Portátiles(Laptop o Tablet)	Equipo personal que puede ser transportado fácilmente, diseñados para soportar software y archivos igual de robustos a los que procesa un computador de escritorio.	Responsable Soporte técnico	Todos los colaboradores asignados con portátiles	**Lugar de residencia.**	No aplica	No aplica	5	ALTO
Hardware (Equipamiento Informático)	APOYO	Infraestructura	A22	Impresora	Máquina que se conecta a una computadora electrónica y que sirve para imprimir la información seleccionada contenida en ella.	Responsable Soporte técnico	Socio Principal jefa de administración y finanzas Business Partner	**Lugar de residencia.**	No aplica	No aplica	1	BAJO
Hardware (Equipamiento Informático)	APOYO	Infraestructura	A23	Dispositivos Móviles(celulares)	Aparato que permite el procesamiento e intercambio de información, la conexión a alguna red, todo esto a través de una memoria interna e ilimitada.	Jefe de administrador y finanzas	Los colaboradores designados con dispositivos móviles	**Lugar de residencia.**	No aplica	No aplica	3	MEDIO

Tabla 18

Inventario de Activos

categoría de activo	proceso	sub proceso	N° de activo	nombre del activo	descripción del activo	propietario	custodio	ubicación física	clasificación	ubicación digital(repositorio)	valor del activo	nivel del activo
Soportes de información	APOYO	Infraestructura	A24	Medios de almacenamiento electrónico (USB, Discos duros externos)	Unidades de almacenamiento externo de información	Business Partner Responsable de soporte técnico	Business Partner Responsable de soporte técnico	No aplica	No aplica	En la ubicación donde se encuentre el responsable del activo (Empleado). **Lugar de residencia.**	3	MEDIO
Colaboradores	APOYO	Gestión de RRHH	A25	Todos los colaboradores	El personal que aporta en cada área de CBC	Business Partner	Jefe de administrador y finanzas	En la ubicación donde se encuentre el responsable del activo (Empleado). **Lugar de residencia.**	No aplica	No aplica	4	ALTO
A. Intangible	APOYO	Infraestructura	A28	Marca Core Business Corp.	Identificador comercial de los bienes y servicios que ofrece CBC.	Jefe de administrador y finanzas	Jefe de administrador y finanzas	No aplica	No aplica	No aplica	1	BAJO

III.3.1.3.1.2.2. Análisis de riesgo

Para realizar el análisis de riesgo se toma en cuenta el resultado del valor del activo, de acuerdo a la siguiente tabla:

Tabla 19

Valor del activo

VALOR	VALOR
ALTO	>=4
MEDIO	[2;4>
BAJO	[1;2>

De acuerdo a el valor que resulte (medio o alto) se realizara el análisis de riesgo.

Para la presente investigación se cuenta con 9 altos, 9 medios y 8 bajos.

III.3.1.3.1.2.2.1. Identificación de Amenazas y vulnerabilidades

De tener un valor de activo de información Media-Alta se identificará las amenazas y vulnerabilidades.

III.3.1.3.1.2.2.2. Cálculo de la Probabilidad

La probabilidad se establece de manera cualitativa, de acuerdo a la siguiente tabla de referencia:

Tabla 20

Probabilidad del riesgo

Valor	Frecuencia	Detalle
3	ALTA	La amenaza ocurrirá siempre o casi siempre
2	MEDIA	La amenaza ocurrirá en algunas ocasiones
1	BAJA	La amenaza ocurrirá raras veces

III.3.1.3.1.2.2.3. Cálculo del Impacto

De materializarse la amenaza identificada se produciría un impacto respecto al activo de información. El cálculo se realiza tomando en cuenta la dimensión afectada definidos en la siguiente tabla de referencia:

Tabla 21

Impacto del riesgo

NIVEL	VALOR	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
ALTA	3	La Falta de disponibilidad puede conllevar a: -Incumplimiento a los acuerdos de nivel de servicio. -Perjuicios legales que afectan la imagen de CBC -Perjuicios económicos.	Información cuya pérdida de exactitud y completitud puede conllevar a un impacto total de índole: -legal a cualquier nivel -Pérdida económica -Perdida de imagen en CBC Afectando la operación de varios de sus procesos y con ello perder de confianza de las partes interesadas.	La divulgación no autorizada de la información puede conllevar un Impacto total de índole legal, operativa, económica o de pérdida de imagen que afecta a todo CBC.
MEDIA	2	La Falta de disponibilidad puede conllevar a: -Afectar los acuerdos -Perjuicios legales que no comprometen a la imagen de CBC -Perjuicios económicos que pueden ser manejados por CBC.	Información cuya pérdida de exactitud y completitud puede conllevar un impacto parcial de índole: - Legal a nivel medio -Pérdida económica o de imagen en CBC Afectando la operación de un proceso especifico.	La divulgación no autorizada de la información puede conllevar un impacto parcial de índole legal, operativa, económica o de pérdida de imagen que afecta a varios procesos de CBC.
BAJA	1	La Falta de disponibilidad no afecta en lo económico, legal y operativo.	Información cuya pérdida de exactitud y completitud conlleva a daños de pequeña magnitud y pérdidas económicas que no afectan las ganancias.	La divulgación no autorizada de la información no conlleva un impacto que afecte al proceso dentro de CBC

III.3.1.3.1.2.2.4. Identificación de las Consecuencias

Se describen las posibles consecuencias que tendrían efecto sobre los activos de información.

III.3.1.3.1.2.2.5. Cálculo del Nivel de Riesgo

El nivel de riesgo es calculado teniendo en cuenta la probabilidad y el impacto, tal como se muestra en la siguiente matriz(ver figura 13):

Figura 9

Nivel de riesgo

NIVEL DE RIESGO		IMPACTO		
		1	2	3
PROBABILIDAD	1	1	2	3
	2	2	4	6
	3	3	6	9

Riesgo - Bajo	[1;2>
Riesgo - Medio	[2;6>
Riesgo - Alto	>=6

III.3.1.3.1.2.3. Tratamiento del riesgo

III.3.1.3.1.2.3.1. Nivel de riesgo aceptable

- El Riesgo será aceptable (de manera automática) si su nivel es Bajo.
- El Riesgo Residual será aceptable (de manera automática) si su nivel es Bajo.

III.3.1.3.1.2.3.2. Estrategias de tratamiento de riesgos

Para tratar cada riesgo no aceptable se ha establecido el siguiente tipo de estrategia:

- Evitar: Core Business tomara medidas encaminadas a prevenir su materialización. Se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resuelto de unos adecuados controles y acciones emprendidas.
- Transferir: el Socio principal reduce su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.
- Mitigar: Esta estrategia consiste en actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo, donde el Socio principal juntamente con el oficial de seguridad de la información seleccionan los controles de seguridad necesarios de acuerdo al anexo A de la norma ISO 27001:2013.
- Aceptar: Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el Comité de Seguridad de la información, puede aceptar el riesgo.

Tabla 22

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	AMENAZA Descripción	VULNERABILIDAD	PROBABILIDAD	IMPACTO D	 I	 C	VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
A2	Divulgación de información	Falla en el control de accesos El personal no tiene claro la función de la gestión de la seguridad de la información	1	2	3	3	2.7	2.7	**MEDIO**	**NO**	Socio Principal	Perdida de información del cliente.	**MITIGAR**
	Fugas de información	Se dejo la laptop encendida con la información a la vista de cualquier tercero.	3	2	3	3	2.7	8.0	**ALTO**	**NO**	Socio Principal	Afectación de la operación de la organización debido a la indisponibilidad de la información.	**MITIGAR**
	Deficiencias en la organización	No se cuenta con políticas de Seguridad de la información	3	3	3	1	2.3	7.0	**ALTO**	**NO**	Socio Principal	Falta de control, revisión, etc.	**MITIGAR**

Tabla 23

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A3	Errores de usuarios	Mal uso de hardware y software	3	1	3	2	2.0	6.0	ALTO	NO	Socio Principal	Perdida de información del cliente.	MITIGAR
	Errores técnicos de TI	No se actualizo el antivirus o software que solicito el Consulto SIG	2	2	3	3	2.7	5.3	MEDIO	NO	Socio Principal	Perdida de información que se le brindara al cliente.	MITIGAR
	Modificación deliberada de la información	Se dejo la laptop encendida con la información a la vista de cualquier tercero.	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Alteraciones, perdida, robo de información que se le brinda al cliente.	MITIGAR

Tabla 24

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A4	Divulgación de información	No contar con una cláusula de confidencialidad de la información.	2	1	3	3	2.3	4.7	MEDIO	NO	Socio Principal	Perdida de información	MITIGAR
	Robo	Estar en lugares públicos Delincuencia No se tienen mecanismos para la seguridad física de activos	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
A5	Perdida de equipos	Descuido del propietario del activo.	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
	Destrucción de la Información	Descuido del propietario del activo.	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR

Tabla 25

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A6	Acceso no autorizado	Ingreso de externos a la nube	2	1	3	3	2.3	4.7	MEDIO	NO	Socio Principal	Perdida de información	MITIGAR
A7	Difusión de software dañino	Correos no deseados con contenido malicioso	2	1	3	3	2.3	4.7	MEDIO	NO	Socio Principal	Ingreso de virus al equipo o dispositivo en uso	MITIGAR
	Errores de encadenamiento	Error de envió de información al destinatario	2	1	3	3	2.3	4.7	MEDIO	NO	Socio Principal	Perdida de información	MITIGAR
A8	Acceso no autorizado	Falta de control de acceso	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
A9	Acceso no autorizado	Falta de control de acceso	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
A10	Acceso no autorizado	Falta de control de acceso	2	1	3	3	2.3	4.7	MEDIO	NO	Socio Principal	Perdida de información	MITIGAR
A11	Suplantación de la identidad del usuario	Personas externas a CBC acceden al control de la página web	1	3	3	3	3.0	3.0	MEDIO	NO	Socio Principal	Mala reputación de CBC con los clientes	MITIGAR

Tabla 26

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A12	Suplantación de la identidad del usuario	Acceso de personal externo	1	3	3	3	3.0	3.0	**MEDIO**	**NO**	Socio Principal		**MITIGAR**
A13	Manipulación de Programas	Vulnerabilidades del app	1	3	3	3	3.0	3.0	**MEDIO**	**NO**	Socio Principal	Desconexión del app	**MITIGAR**
A18	Difusión de software dañino	Descargar software desconocidos que contienen virus	1	3	3	1	2.3	2.3	**MEDIO**	**NO**	Socio Principal	Mala reputación de CBC con los clientes	**MITIGAR**
A19	Errores técnicos de TI	Licencia caducada	1	1	3	3	2.3	2.3	**MEDIO**	**NO**	Socio Principal	Ingreso de virus a laptop, Tablet, entre otros	**MITIGAR**

Tabla 27

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A21	Robo	Descuido del propietario del activo Delincuencia	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Pérdida Total del portátil	MITIGAR
	Errores de usuarios	Dejar la información en carpetas que están a la vista de todos No se cuenta con contraseñas	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Robo de Información Acceso a información no autorizada Inserción de data corrupta	MITIGAR
	Errores de mantenimiento	No se realiza el mantenimiento adecuado a los equipos Antigüedad del Equipo Mantenimientos No Son Planificados	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
	Fuego	Descuido del propietario del activo	3	3	2	1	2.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
	Daños por agua	Descuido del propietario del activo	3	3	2	1	2.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR

Tabla 28

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A23	Robo	Descuido del propietario del activo Delincuencia	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Pérdida de clientes debido a la sustracción y divulgación no autorizada de información confidencial alojada en el aplicativo de gestión documental.	MITIGAR
	Errores de usuarios	Dejar sin Pin, contraseña los celulares de uso para CBC No existe una política de dispositivos móviles	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Perdida de información	MITIGAR
	Errores de usuarios	No existe una gestión de medios removibles	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Pérdidas de información	MITIGAR
A24	Robo	Descuido del propietario del activo Delincuencia	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Pérdida del medio de almacenamiento	MITIGAR

Tabla 29

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A25	Indisponibilidad del personal	El colaborar se encuentra indispuesto debido a un accidente, incidente o situaciones personales	2	3	1	1	1.7	3.3	**MEDIO**	**NO**		Perder proyectos por ausencia de personal	**MITIGAR**
	Deficiencias en la organización	No se especifican los roles y requerimientos relacionados a SI en la etapa de selección del colaborador	2	2	2	2	2.0	4.0	**MEDIO**	**NO**	Socio Principal	Incumplimiento de las política de excelencia organizacional	**MITIGAR**
	Abuso de privilegios de acceso	No existe un proceso disciplinario Incumplimiento de permisos, privilegios y control de acceso	2	2	2	2	2.0	4.0	**MEDIO**	**NO**	Socio Principal	No se cuentan con un proceso disciplinario	**MITIGAR**
	Fugas de información	No se quita accesos a los colaboradores que han culminado su contrato	2	2	2	2	2.0	4.0	**MEDIO**	**NO**	Socio Principal	Perdida de información y confianza por parte del cliente	**MITIGAR**

Tabla 30

Matriz de riesgo

IDENTIFICACIÓN DE ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO			VALOR IMPACTO	RIESGO	NIVEL DE RIESGO	¿RIESGO ACEPTABLE?	PROPIETARIO DEL RIESGO	CONSECUENCIAS	TRATAMIENTO
N° DE ACTIVO	Descripción			D	I	C							
A25	Uso no previsto	Utilizan hardware para uso personal	3	2	2	2	2.0	6.0	ALTO	NO	Socio Principal	Uso inapropiado de equipos	MITIGAR
	Divulgación de información	No se cuenta con política de medios removibles	2	2	2	3	2.3	4.7	MEDIO	NO	Socio Principal	Perdida de información y confianza por parte del cliente	MITIGAR
	Extorsión	Delincuencia	2	3	3	3	3.0	6.0	ALTO	NO	Socio Principal	Robo de Información Acceso a información no autorizada Inserción de data corrupta	MITIGAR
	Deficiencias en la organización	No se definió adecuadamente las responsabilidades de los colaboradores	1	1	2	3	2.0	2.0	MEDIO	NO	Socio Principal	Falta de control, revisión, etc.	MITIGAR

III.3.1.3.1.2.4. Selección de controles de seguridad

Para cada amenaza cuyo nivel de riesgo no es aceptable se realiza la descripción de las acciones con el propósito de realizar el tratamiento en base a la estrategia elegida. (ver tabla 27)

El propietario del riesgo estará a cargo de la realización de los controles tomados.

De acuerdo a los controles establecidos en el Anexo de la norma ISO 27001.

Para el cálculo del riesgo residual, al culminar con el tratamiento y los controles implementados se analizará el riesgo residual de la misma forma que se hizo al inicio con la evaluación de riesgo.

De la misma manera, para dar seguimiento y revisión del Tratamiento de Riesgos, el socio principal juntamente con el Business Partner dan seguimiento a los controles tomados para cada activo no aceptable. (ver tabla 31)

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A2	Información del cliente	**MITIGAR**	A.13.2.4 Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados. *Actualizar el FOR. 036 compromiso de Seguridad de la información *FOR.049 Compromiso de confidencialidad de los colaboradores *compromiso de confidencialidad para el cliente(listado de personal)
			A.9.1.1 Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. *Elaborar y comunicar/concientizar una política de control de acceso
			A.15.1 Seguridad de la información en las relaciones con los proveedores	Asegurar protección a los activos de la organización que son accesibles por los proveedores *Elaborar una política de proveedores *Contar con acuerdos
		MITIGAR	A.11.2.9 Política de escritorio limpio y pantalla limpia	*FOR.049 Compromiso de confidencialidad de los colaboradores
		MITIGAR	A. 5.1.1 Política de seguridad de la información	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A3	Informes de proyectos	**MITIGAR**	A.12.6.2 Restricciones sobre la instalación de software	*Elaborar y comunicar/concientizar una política de control de acceso
			A.12.2.1 Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios
		MITIGAR		*Elaborar una política prohibiendo el uso de software no autorizado e implantación de controles que prevengan o detecten el uso de software no autorizado
			A.12.3.1 Respaldo de la información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada. *Establecer una política de respaldo, y probar copias de información de software y del sistema.
		MITIGAR	A.9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso *Concientizar con una política de control de acceso
A4	Contratos	**MITIGAR**	A.13.2.4 Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados. *Revisar y actualizar si es el caso los acuerdos, y comunicarlos a todos los colaboradores y proveedores.

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A5	Copias de respaldo de Información de CBC	**MITIGAR**	A.17.1.2 Implementación de continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa. *Elaborar un Plan de contingencia
			A.16.1 Gestión de incidentes de seguridad de la información y mejoras	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades *Elaborar un procedimiento de gestión de incidentes
		MITIGAR	A.11.2.8 Equipos de usuario desatendidos	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada *Elaborar un comunicado sobre la seguridad en lugares públicos y protección del equipo con contraseñas seguras
		MITIGAR	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.(métodos criptográficos) *Elaborar un comunicado sobre la seguridad en lugares públicos
			A.8.3.1 Gestión de medios removibles	*Elaborar y comunicar una política/procedimiento de Gestión de medios removibles

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A6	Copias de respaldo de Información a nivel de usuario	**MITIGAR**	A.9.2 Gestión de acceso de usuario	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios. *Elaborar y comunicar la política de control de accesos *Elaborar y comunicar la política de escritorio y pantalla limpia
		MITIGAR	A.12.2 Protección contra códigos maliciosos	Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos. *Comunicar sobre el buen uso de correo corporativo
A7	Mensajería(Correo corporativo)	**MITIGAR**	A.13.2 Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. *Elaborar y comunicar una política de transferencia de información *Comunicar sobre el buen uso de correos corporativos y el cuidado con los enlaces sospechosos
			A.13.2.1 Políticas y procedimientos de transferencia de la información	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.
A8	MS SharePoint Online	**MITIGAR**	9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones. *Verificar que los colaboradores asignados tengan los accesos al Share Point *Comunicar sobre repositorio de información
A9	Google drive	**MITIGAR**	9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones. *Verificar que los colaboradores asignados tengan los accesos al drive *Comunicar sobre repositorio de información
A10	Elea ring-Intranet	**MITIGAR**	9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos a la plataforma de E-learning-intranet

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A11	Página Web	**MITIGAR**	9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos a la plataforma de E-learning-intranet
A12	Outlook	**MITIGAR**	9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos para el uso correcto de Outlook
A13	Power Apps	**MITIGAR**	A.14.2 Seguridad en los procesos de desarrollo y soporte	Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A18	Microsoft Windows(Sistema Operativo)	**MITIGAR**	A.12.1 Procedimientos y responsabilidades operativas	Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.
A19	Antivirus	**MITIGAR**	A.12.2 Protección contra códigos maliciosos	Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos *Cada colaborar que cuente con laptop, tablep deben contar con un antivirus confiable, y actualizado.

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A21	Portátiles(Laptop o Tablet)	**MITIGAR**	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización *Elaborar un comunicado sobre la seguridad en lugares públicos y protección del equipo con contraseñas seguras
		MITIGAR	A.9.1.1 Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. *Se elaborará y comunica una Política de control de accesos
			A.11.2.1 Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
		MITIGAR	A.11.2.9 Política de escritorio limpio y pantalla limpia	Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada. *Comunicar la política de escritorio y pantalla limpia
		MITIGAR	A.11.2.4 Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. *Elaborar un procedimiento de Mantenimiento de equipos *Programar y ejecutar los mantenimientos preventivos (anual)
		MITIGAR	A.16.1 Gestión de incidentes de seguridad de la información	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades. *Comunicar la política de escritorio y pantalla limpia
		MITIGAR	A.16.1 Gestión de incidentes de seguridad de la información	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades. *Comunicar la política de escritorio y pantalla limpia

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A23	Dispositivos Móviles(celulares)	**MITIGAR**	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. *Elaborar una política de Trabajo remoto
			A.11.2.1 Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
		MITIGAR	A.6.2.1 Política de dispositivos móviles	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles. *Elaborar un Plan de contingencia *Comunicar la política de dispositivos móviles
A24	Medios de almacenamiento electrónico (USB, Discos duros externos)	**MITIGAR**	A.8.3.1 Gestión de medios removibles	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización. *Elaborar y comunicar una política/procedimiento de Gestión de medios removibles
		MITIGAR	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. *Comunicar el Plan de contingencia

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A25	Todos los colaboradores	**MITIGAR**	A6.1 Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. *Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto
		MITIGAR	A.7.1 Antes del empleo	Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera. *Verificar los antecedentes Penales, policiales y judiciales de todos los colaboradores *Entregar las políticas de SI *Contar con los acuerdos, contratos, entre otros documentados
		MITIGAR	A.7.2 Durante el empleo	Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información. *Dar a conocer las responsabilidades en la inducción *Brindar capacitaciones, comunicaciones relacionadas a seguridad de la información *Elaborar y comunicar un proceso disciplinario
		MITIGAR	A.9.2 Gestión de acceso de usuario	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.
		MITIGAR	A.7.3 Terminación y cambio de empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo *Levantar las actas de devolución de activos al término del contrato *si es cambio de responsabilidades, brindar y acceso adecuado
		MITIGAR	A.8 Gestión de activos	Identificar los activos de la organización y definir responsabilidades de protección apropiadas Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización. *Elaborar el procedimiento de gestión de activos y comunicar sobre las buenas prácticas de seguridad de información
		MITIGAR	A.6.2.2 Trabajo remoto	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo. *Elaborar y comunicar una política de trabajo remoto

Tabla 31

Tratamiento SI

IDENTIFICACIÓN DE ACTIVO		TRATAMIENTO	CONTROL	ACCIONES A TOMAR
N° DE ACTIVO	NOMBRE DEL ACTIVO			
A25	Todos los colaboradores	**MITIGAR**	A.8.3 Manejo de los medios	Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios. *Comunicar la política de medios removibles
			A.13.2.4 Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.
		MITIGAR	A.17.1 Continuidad de seguridad de la información	La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización Elaborar y comunicar el plan de contingencia de SI Elaborar planes de respuesta ante emergencia (continuidad)
		MITIGAR	A.6.1.Organización interna	La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización *Actualizar el MOF *Elaborar la política de gestión de activos(con las responsabilidades del propietario del activo, custodio y propietario del riesgo) *Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto *Concientizar sobre la importancia de un Sistema de Gestión de la información *Selección y comunicación del cargo de Oficial de seguridad de la información *Concientizar sobre la seguridad de la información

III.3.1.3.2. Objetivos de seguridad de la información y planificación para conseguirlos

CBC ha establecido objetivos para las funciones y niveles pertinentes (ver tabla 36) y los procesos detallados en el POL.008. Caracterización de procesos. (ver anexo 8)

Los objetivos son:

a. Coherentes con la política de excelencia organizacional y políticas SI

b. Medibles.

c. Consideran los requisitos aplicables.

d. Comunicados por los comités internos.

e. Actualizados, según corresponda.

Tabla 32

Objetivos

Política	Objetivo	Indicadores	Meta	Formato / Fuente de datos	Frecuencia de medición	Responsable
Preservar la confidencialidad, integridad y disponibilidad de la información de nuestras partes interesadas.	Controlar los riegos de información en los proceso de la empresa	RIESGOS SI. Control operacional: (N° acciones ejecutadas del Control Operacional del RIEGOS SI/ Total de acciones) x 100%	70%	Matriz de RIESGOS SI	Mensual	Procesos SIG/ Business Parte
	Controlar las amenazas en la seguridad de la información	% de ataques informáticos que impidieron la prestación de algún servicio	0	Registros de incidencias	Mensual	Procesos SIG/ Business Parte

Resumen del formato FOR.002

III.3.1.4. Soporte

III.3.1.4.1. Recursos

CBC determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua, mediante el FOR.003 Programa anual (ver anexo 9), el cual considera:

- Recurso humano: MAN.001 Manual de Organización y Funciones, FOR.016. Programa anual de capacitación y FOR.032. Organigrama.
- Recurso tecnológico: mediante el FOR.034. Inventario de equipos tecnológicos.
- Recurso económico: mediante documentos internos del área de administración y finanzas.

III.3.1.4.2. Competencia

CBC:

a) Determina la competencia necesaria mediante el MAN.001 Manual de Organización y Funciones. (ver anexo 12)
b) Se asegura que los colaboradores son competentes, mediante:
    - Selección de personal, mediante el procedimiento de PRO.009 Gestión de Recursos Humanos.(ver anexo 18)
    - Cumplimiento del FOR.016. Programa anual de Capacitación.(ver figura 14)
    - FOR.018. Evaluación de desempeño.(ver anexo 19)
    - Cumplimiento de los FOR.002 Objetivos e indicadores del SIG (ver anexo 6)

c) Cuando sea aplicable, se implementa acciones para adquirir la competencia mediante el procedimiento PRO.008 Capacitación.(ver anexo 20)

III.3.1.4.3. Concientización

CBC mediante capacitaciones, comunicaciones, inducciones y comités de seguimiento se asegura que los colaboradores tomen conciencia de:

- La POL.001 Política de Excelencia Organizacional y política de Seguridad de la información.
- Los FOR.002 Objetivos e indicadores del SIG
- Las implicaciones del incumplimiento de los requisitos del Sistema de Gestión de la información.

Figura 10

Formato de Plan anual de capacitaciones

	FORMATO	CODIGO: FOR.016
Core Business corp.	PLAN ANUAL DE CAPACITACIONES	VERSIÓN: 02 Fecha: 05/10/2021

TEMA	Objetivo	DICTADO POR	Publico Objetivo	Set	Oct	Nov	Dic	Estado
Sistema de Gestión de Información ISO 27001:2013	Conocer los pincipales lineamientos de la ISO 27001:2013.	CHRISTIAN MATOS	Todos					EJECUTADA
Identificación de Peligros, Evaluación de Riesgos y Toma de controles	Conoce los lineamientos del IPERC	PAUL ALIAGA	Todos					EJECUTADA
Gestión de riesgos en seguridad de la información	Conocer los principales riesgos en seguridad de la información	JOSE LUIS SANDOVAL	Todos					EJECUTADA
Matriz de requisitos legales	Conocer los requisitos legales	JEREMY VELÁSQUEZ	Todos					EJECUTADA
Investigación de inccidentes	Conocer las causas más comúnes de accidentes y cómo evitarlos.	MIRELLA AUCAPIÑA	Todos					EJECUTADA
Buenas practicas de auditorias e inspecciones. Taller	Conocer el procedimiento de inspecciones y auditoria.	ISABEL HUAPAYA	Consultores					EJECUTADA
% DE CUMPLIMIENTO				100%	100%	100%		

III.3.1.4.4. Comunicación

CBC determina las comunicaciones internas mediante el FOR.033. Programa Anual de Comunicación y sensibilización (ver figura 15) y externas (POL.007 Plan de comunicaciones). Las comunicaciones se evidencian en el anexo 21.

Figura 11

Programa de comunicaciones y sensibilización interna

	FORMATO				Código: FOR.032				
	PROGRAMA ANUAL DE COMUNICACION Y SENSIBILIZACIÓN				Fecha: 16/03/2021				VERSIÓN: 2
LINEAMIENTO	MEDIO DE COMUNICACIÓN	RESPONSABLE	ALCANCE	PROGRAMA				% CUMPLIMIENTO
				Sep	Oct	Nov	Dic	
COVID19	Correo, Whatsapp	Administración y Finanzas	Colaboradores					100%
Teletrabajo	Correo, WhatsApp	Administración y Finanzas	Colaboradores					100%
Objetivos (SIG)	Comité Interno	Socio Principal	Colaboradores					100%
Política de Excelencia Organizacional y Politicas SI	Correo, Web	Administración y Finanzas	Colaboradores, Clientes, proveedores, todos					100%
Procesos y Gestión de Riesgos	Correo	Administración y Finanzas	Colaboradores					100%
Cuidado de la información	Correo	Administración y Finanzas	Colaboradores					100%
Importancia del Sistema de Gestión de Seguridad de la información.	Correo	Administración y Finanzas	Colaboradores					100%
Consejos para proteger la información de medios digitales.	Correo	Administración y Finanzas	Colaboradores					100%
Buenas prácticas para un Sistema de Gestión de Seguridad de la información.	Correo	Administración y Finanzas	Colaboradores					100%
Rol del Consultor (Trabajo en equipo)	Correo	Administración y Finanzas	Colaboradores					100%
Protege tu equipo con contraseña segura.	Correo	Administración y Finanzas	Colaboradores					100%
Repositorio de información	Correo	Administración y Finanzas	Colaboradores					100%
Da buen uso a los correos corporativos.	Correo	Administración y Finanzas	Colaboradores					100%
Ten cuidado con los enlaces sospechas.	Correo	Administración y Finanzas	Colaboradores					100%
No deje información delicada a la vista.	Correo	Administración y Finanzas	Colaboradores					100%
TOTAL INTERNO				100.00%	100.00%	100.00%	100.00%	100.00%

III.3.1.4.5. Información documentada

En la Lista Maestra se encuentra la información documentada, incluye:

a. La información documentada requerida por la ISO 27001 tales como: alcance, mapa de procesos, lista de requisitos de servicio, política de excelencia organizacional, objetivos, entre otros.
b. la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de la calidad

CBC cuenta con el procedimiento para el control de la información documentada denominado: PRO.001 – Control de Información Documentada (ver anexo 22) el cual establece las tareas de:

a. Creación o actualización, donde se considera
    - La identificación y descripción.
    - El formato y los medios de soporte.
    - La revisión y aprobación con respecto a la conveniencia y adecuación
b. Control:
    - Todos los documentos están almacenados en la carpeta SharePoint, la cual está compartida con todos los colaborares de la organización.
    - Los documentos de origen externo son registrados en la Lista Maestra de Información Documentada. Las versiones obsoletas o antiguas de los documentos son identificadas en una carpeta “DOCUMENTOS OBSOLETOS”. Ubicado en la carpeta del SharePoint.
    - Los documentos identificados como registros son almacenados en la carpeta compartida de SharePoint.

- CBC controla los cambios de la documentación según lo detalla el procedimiento PRO.004 – Gestión del cambio. (ver anexo 23)
- CBC cuenta con un respaldo digital (recuperación) de todos los documentos del SIG de acuerdo con el procedimiento PRO.015 - Infraestructura tecnológica. (Anexo 24)

III.3.2. Hacer

Dentro de esta etapa hacer se hará uso del requisito 8 de la normativa ISO 27001:2013.

III.3.2.1. Operación

III.3.2.1.1. Planificación y control operacional

CBC planifica, implementa y controla los procesos necesarios para cumplir con los requisitos del sistema de información e implementa las acciones determinadas en el análisis de riesgos y oportunidades.

La determinación, mantenimiento y conservación de la información documentada está gestionada en los procedimientos operativos, PRO.001 Control de Información Documentada (ver anexo 22) y PRO.015 Infraestructura Tecnológica, los cuales:

- Brindan confianza en que los procesos se han llevado a cabo según lo planificado.
- Demuestran la conformidad de los productos y servicios con sus requisitos.

III.3.2.1.2. Evaluación de riesgos de seguridad de la información

Para la evaluación de riesgos se realizó el procedimiento PRO.023 Procedimiento de Gestión de riesgos operacionales. (ver anexo 17)

III.3.2.1.3. Tratamiento de riesgos de seguridad de la información

CBC implementar el plan de tratamiento de riesgos de seguridad de la información mediante los controles del anexo A de la norma.(ver tabla 34)

III.4. Objetivo 4. Evaluar el desempeño de la seguridad de información de la empresa CBC

III.4.1. Verificar

Dentro de esta etapa verificar se hará uso del requisito 9 de la normativa ISO 27001:2013.

III.4.1.1. Evaluación del desempeño

III.4.1.1.1. Monitoreo, medición, análisis y evaluación

CBC determina:

a) qué necesita seguimiento y medición: FOR.002. Objetivos e indicadores del SIG.
b) Los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos, mediante comités internos, encuestas de satisfacción del cliente, evaluación de proveedores.
c) Cuando se deben llevar a cabo el seguimiento y la medición establecidos en el FOR.002. Objetivos e indicadores del SIG y en la POL.008. Caracterización de Procesos

d) Cuando se deben analizar y evaluar los resultados del seguimiento y la medición, en Comités y Revisión por la Dirección.

La organización evalúa el desempeño y la eficacia del sistema de gestión de la información en los Comités y Revisión por la Dirección y mediante actas se evidencia su cumplimiento.

III.4.1.1.2. Auditoría interna

CBC ha determinado un procedimiento PRO.003 Gestión de Auditoría (ver anexo 25) FOR.009 Programa Anual de Auditoria y FOR.010 Plan de Auditoria la planificación de las auditorias referente al sistema de gestión, en donde se establecen:

- Los requisitos propios de la organización para su sistema de gestión de la información.
- Los requisitos de esta Norma Internacional.
- CBC planifica, establece, implementa y mantiene un programa de auditoría que incluye la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que tiene en consideración la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorias previas, mediante PRO.003 – Gestión de Auditoria, en FOR.009 Programa Anual de Auditoria y FOR.010– Plan de Auditoria (ver anexo 26)
- CBC define los criterios de la auditoria y el alcance para cada auditoria en el formato FOR.010 - Plan de auditoría.

- CBC selecciona los auditores y lleva a cabo auditorias para asegurarse de la objetividad y la imparcialidad del proceso, mediante el procedimiento PRO.011 - Gestión de Proveedores.(ver anexo 27)
- CBC se asegura de que los resultados de las auditorias se informen a la dirección pertinente, según lo mencionado en el procedimiento PRO.003 – Gestión de Auditoria.
- CBC realiza las correcciones y toma las acciones correctivas adecuadas sin demora injustificada según lo descrito en el procedimiento PRO.002 Tratamiento de No Conformidad y Acción Correctiva.

CBC conserva información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorias mediante el formato FOR.011 informe de auditoría interna.

III.4.1.1.3. Revisión por la gerencia

La revisión por la dirección lo realiza la alta dirección por lo menos una vez cada semestre y/o cuando se estime conveniente de acuerdo a las necesidades de seguimiento y control del SGSI. Las entradas y salidas están definidas en el procedimiento PRO.007 – Revisión por la Dirección. (ver anexo 28)

III.4.2. Actuar

Dentro de esta etapa Actuar se hará uso del requisito 10 de la normativa ISO 27001:2013.

III.4.2.1. Mejora

III.4.2.1.1. No conformidades y acción correctiva

CBC toma acciones para controlar y corregir las no conformidades detectadas según el procedimiento PRO.002 – Tratamiento de No Conformidad y Acción Correctiva(ver anexo 29) y formato FOR.006 – Registro de Acción Correctiva en donde se incluyen:

- La revisión y el análisis de la no conformidad.
- La determinación de las causas de la no conformidad.
- La determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir.
- La revisión de la eficacia de cualquier acción tomada.
- La actualización de la Matriz de Riesgos y Oportunidades, en caso fuese necesario.
- La realización de cambios según el procedimiento PRO.004 – Gestión del Cambio, en caso fuese necesario.

CBC conserva evidencia de las acciones tomadas. Estas son registradas en el formato base de datos de acción correctiva (ver anexo 30).

III.4.2.1.2. Mejora continua

Se ha establecido procesos para mejorar continuamente el desempeño del SI, a través de la Política de Excelencia Organizacional y políticas SI, Objetivos e Indicadores del SIG, resultados de auditorías, análisis de datos, gestión de riesgos y oportunidades, acciones correctivas y revisión por la dirección. Los cuales son canalizados por el procedimiento PRO.002 – Tratamiento de No Conformidad y Acción Correctiva.

III.5. O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013.

Al culminar con la implementación de acuerdo a los capítulos 4 al 10 de la norma ISO 27001:2013 el día 9/11/2021. Se realizó la verificación de cumplimiento de controles entre el 9/11/2021 al 24/11/2021 que resulto de la matriz de riesgos se SI (ver anexo 31).

Entre el día 24/11/2021 al 26/11/2021 se hizo uso de la lista de verificación para corroborar el cumplimiento de la norma ISO 27001:2013, en el cual resulto contar con un 100%. (ver tabla 41)

Tabla 33

Cumplimiento de la implementación

CAPITULO	% POR CAPITULO	SIGNIFICADO
4	**100%**	Las actividades han sido validadas y muestran mejoras
5	**100%**	
6	**100%**	
7	**100%**	
8	**100%**	
9	**100%**	
10	**100%**	
TOTAL	100%	

IV. CAPÍTULO. DISCUSIÓN Y CONCLUSIONES

IV.1. Alcance

La implementación de la norma ISO 27001:2013 (SGSI) beneficia a toda la organización, específicamente al proceso operativo de la empresa, sin embargo, a los demás procesos, como el de apoyo y estratégico están limitados estrictamente a un sub conjunto de procesos los cuales han sido declarados dentro del alcance del SGSI.

IV.2. Limitaciones

La Información se logró recopilar gracias a la facilidad que brindo la empresa Core Business Corporation SAC entre los meses de agosto a noviembre del año 2021. Asimismo, debido a un trabajo remoto se cuenta con una comunicación limitada, pero ya que la alta gerencia tiene el propósito de cumplir con la implementación, hubo un apoyo, permitiendo así la implementación de la norma ISO 27001:2013.

IV.3. Interpretación comparativa

A nivel mundial, los robos cibernéticos son una forma de delincuencia transnacional y uno de los que crecen cada año, este delito afecta a más de 431 millones de víctimas adultas a nivel mundial.(Jan, s. f.). Al igual que en el Perú la herramientas de ciberacoso y espionaje ha aumentado un 145% en el 2020 en adelante. (Gascón, 2021) Podemos inferir que a medida que la tecnología avanza, crecen las amenazas de perdida de información de todo tipo. Es por ello, que las empresas deben asumir una responsabilidad y contar con mecanismos para proteger la información con la que cuentan.

Hoy en día es posible una certificación de la ISO 27001:2013, la cual permite contar con una gestión adecuada para proteger a los activos de información y de esta manera contar con beneficios como la reputación de la organización, compromiso, mitigación de riesgos de SI, entre otros.

Entre enero y abril del 2021 en el Perú, se investigaron 1,188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía. Los casos más frecuentes desde el año 2015 hasta la actualidad están relacionados al fraude informático y a la suplantación de identidad, es por ello que es importante que las organizaciones cuenten con controles adecuados, optimicen sus sistemas de información, y brinden de esta manera a sus clientes confidencialidad.

Para realizar una comparación se tomó en cuenta a los antecedentes, analizando cada una de ellas y dando a conocer el aporte que dio a la presente investigación.

Yagual del Valle y Rodríguez (2014), en su tesis titulada "Análisis para la integración de un sistema de Gestión de Seguridad de Información (SGSI) ISO 27001 utilizando OSSIM para empresa industrial", hizo uso del método de investigación de riesgo de Magerit, el cual permitió realizar la matriz de riesgo, determinando que tan expuesto se encontraba un activo de información. El cual le permitió identificar 15 riesgos que podrían afectar a 18 procesos críticos, para cada riesgo se seleccionaron los controles adecuados referentes al anexo A de la norma ISO 27001.

Torres (2020), en su tesis titulada "Plan de Seguridad Informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A". Concluyo que un Sistema de Gestión de la Seguridad de la información aplicado mediante la norma internacional ISO 27001 permite tomar conciencia sobre la importancia que tiene la seguridad de la información, además, fue de vital importancia

contar con una matriz de riesgos, la cual ayudo a identificar las vulnerabilidades existentes en los activos de información, el cual se desarrolló gracias a la metodología MAGERIT permitiendo identificar la probabilidad e impacto de riesgos a los que se pueden enfrentar los activos de información, para poder emplear los controles necesarios y así mitigar los riesgos existentes.

Para la presente investigación se hizo uso de la misma metodología de Magerit que ambos autores anteriormente mencionados utilizaron. En el caso de Core Business Corporation se realizó la matriz de riesgos operacionales de SI, el cual arrojo 28 activos de información de las cuales solo 18 fueron analizados para asumir un tratamiento y tomar controles adecuados según el anexo A de la norma ISO 27001:2013.

Córdoba (2021), en su tesis titulada "Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia". Identificaron que los requerimientos que exige la Norma ISO 27001:2013 y la Ley 1581 sirvieron para el cumplimiento de la protección de datos personales, también alerta sobre los riesgos administrativos y económicos que conllevaría para la institución universitaria el no cumplimiento. Esto permite inferir que existe un beneficio para la organización al contar con una implementación de la ISO 27001:2013, dando un beneficio no solo económico, sino también contar con una reputación y así fidelizar a sus clientes, y en un corto plazo contar con una cartera más atractiva logrando posicionarse en el mercado.

Vilca (2017), en su tesis titulada "Diseño e Implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de lima". Logró optimizar los procesos de capacitación y de formación de la

seguridad en cuanto al uso de la información de la empresa, al uso de los equipos de la empresa y el uso de la información. En esta tesis se infiere que una implementación de la ISO 27001:2013 aporta no solo a una área TI sino también puede realizarse para mejorar diversas áreas que involucren activos de información. Esto permite a muchas organizaciones utilizar controles del anexo A de la norma ISO 27001:2013 aplicadas a su organización, no quiere decir que deberían cumplir con todas, sino utilizar ciertos controles de acuerdo a su contexto.

Llanos y Elías (2016), en su tesis titulada "Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software". En una de sus conclusiones menciona que para elaborar una implementación y cumplir los requisitos del estándar 27001 deben considerarse aquellos estándares que forman parte del dominio de algunos de los requisitos del SGSI, esto ayuda a muchas organizaciones apoyarse de otras normas que probablemente no sean certificadas pero que aportan a desarrollar adecuadamente una implementación, como la ISO 31001 de gestión de riesgos, ISO 27002 Practicas para los controles de seguridad de la información, entre otras.

Vásquez (2018), en su tesis titulada "Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI". Menciona que la norma ISO 27001:2013 puede integrarse a las diversas normas debido a su estructura a las demás normas ISO 9001, ISO 14000, etc., asimismo, debido a que el personal es un factor importante y es quien opera en su mayoría los procesos del negocio, es necesario que esté capacitado en temas técnicos para la operación del proyecto y concientizado en la importancia de la seguridad de la información y en que sus actividades contribuyen a la protección de la información. Cabe indicar que Core Business Corporation cuenta con una

certificación de la norma ISO 9001:2015 haciendo posible una integración con la norma ISO 27001:2013, permitiendo así contar con una gestión integrada que permite monitorear los procesos y salvaguardar no solo a los clientes sino a la información que transita en diversos medios como documentos digitales, informes del cliente, discos duros que mantienen dicha información, laptops y celulares que cuentan con información sensible, entre otros.

Benites (2019), en su tesis titulada "Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza". Se infiere que el desarrollo del plan de Implementación de un SGSI requiere de un trabajo, esfuerzo y gran desempeño de toda una organización, asimismo, la ejecución de los controles, políticas, metodologías y estrategias planteadas en el desarrollo del SGSI viene acompañada del compromiso de todos los colaboradores ya que son los responsables del resultado del SGSI. Gracias a la colaboración continua por parte de la alta gerencia de Core Business Corporation se desarrolló de manera rápida y fluida la implementación ISO 27001:2013, ya que cabe recalcar que esta puede tardar entre 6 meses a 1 año, claro que se culmina con una certificación. Por ser esta una investigación de implementación se acorto el tiempo a 4 meses de acuerdo al cronograma que se estableció con todo el comité de la organización.

Mediante los antecedentes mencionados en el capítulo I, cada autor llego en su análisis que la norma ISO 27001:2013 ayuda a optimizar los procesos, controlar y proteger a los activos de información de la organización, brindando beneficios como la reputación, mitigación de amenazas y riesgos de seguridad de la información, compromiso, entre otros.

.

Además, se observó mediante la lista de verificación que la organización Core Business Corporation SAC antes de la implementación contaba con un 39% de cumplimiento, y al termino se volvió a evaluar llegando a un 100% de cumplimiento de la norma ISO 27001:2013, lo cual fue satisfactorio para la organización.

Como resultado del desarrollo de la investigación, se concluye que se logró dar respuestas a los objetivos del presente proyecto:

- **O1: Elaborar el diagnóstico situacional de la empresa Core Business Corporation SAC**

Mediante al uso del instrumento (lista de verificación) se verifico que al inicio Core Business Corp. contaba con un 39% de cumplimiento de la norma ISO 27001:2013, esto quiere decir que cumplía con ciertos lineamientos de la norma mas no tenía una gestión adecuada, por ello se realiza la implementación, dando lugar a que cumpla al 100%.

- **O2: Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013.**

El análisis de costo/ beneficio, permitió a Core Business Corporation organizarse de manera estratégica contando con una inversión que conlleva a una certificación de la ISO 27001:2013, además, se cuenta con un costo que está sujeto a los recursos que se necesitó para dicha implementación y certificación , en cuanto al beneficio, este está relacionado al ahorro en pérdidas económicas que genera los posibles incidentes de seguridad de la información y penalidades por parte de los clientes, además de los beneficios de reputación y los mencionados en el capítulo de resultados. Debido a que el costo/beneficio resulto 1.96, siendo el beneficio mayor que el costo, la implementación de la norma ISO 27001:2013 es rentable. Así se concluye que la implementación mejora la

reputación, disminuye las amenazas de SI y se cumplen con las leyes legales y contractuales de los clientes.

- **O3: Elaborar el análisis de riesgo de seguridad de la información.**

El ciclo PHVA permitió un desarrollo adecuado, cumpliendo con cada requisito pertinente de la norma ISO 27001:2013 (capitulo 4,5,6,7 y 8), dando respuesta al objetivo presente.

Donde se hizo uso del FODA, el cual evidencio la existencia de amenazas como ataques cibernéticos, perdida de información y errores de software y como oportunidad de mejora al avance tecnológico y personal competente en Sistema de Gestión. Además, se identificó a las partes interesadas y con ello se estableció el alcance del SGSI.

También, se hizo uso de la metodología de Magerit, donde se identificaron a los activos de información más relevantes de la organización, contando con 9 activos de nivel altos, 9 medios y 8 bajos teniendo un total de 26 activos de información. A continuación, se realizó el análisis de riesgo de la seguridad de la información de los activos que tuvieron un nivel de riesgo medio-alto. Con ello se realizó la matriz de Gestión de riesgos operacionales de SI, que permitió identificar las amenazas y vulnerabilidades y el nivel de riesgo relacionadas a los activos de información. Contando con 38 riesgos de SI entre medio y alto. Además, se utilizó el tratamiento de mitigar (reducir) los riegos de nivel medio y alto haciendo uso de los controles del anexo A de la norma ISO 27001:2013.

Para el desarrollo de lo mencionado anteriormente, a la par Core Business Corporation determino y proporciono los recursos humanos, tecnológicos y económicos, así como un reclutamiento adecuado, sensibilizando a sus colaboradores mediante capacitaciones y comunicaciones relacionadas a SI.

❖ **O4: Evaluar el desempeño de la seguridad de información de la empresa Core Business Corporation SAC**

El ciclo PHVA permitió un desarrollo adecuado, cumpliendo con cada requisito pertinente de la norma ISO 27001:2013, dando respuesta al objetivo presente. (capitulo 9 y 10)

Al inicio del proyecto se tenía un 58% y 50% de cumplimiento de la norma ISO 27001:2013 de los capítulos 9 y 10 respectivamente. Significando que las actividades han sido identificadas y desarrolladas, pero no se ajustaban plenamente a la norma o están implementadas parcialmente. Posterior a la implementación se obtuvo una mejora significativa del 100% de cumplimiento de la norma ISO 27001:2013.

Además, mediante el monitoreo de los objetivos de seguridad de la información, reuniones de comité SI, programas de comunicaciones y sensibilizaciones se logra verificar el cumplimiento del desempeño. Esta se mantendrá en el tiempo mejorando continuamente, logrando así un sistema de gestión de seguridad de la información adecuada.

❖ **O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013**

Al término de la implementación se hizo uso de la lista de verificación, del cual se obtuvo un 100% de cumplimiento de la norma ISO 27001:2013, y adicionalmente se evidenciaron los controles establecidos que reducen el nivel de riesgo, contando así con 30 riesgos bajos, 8 medios los cual mejoraran de manera continua.

V. REFERENCIAS

Benites Durand, C. A. (2019). Implementación de un sistema de gestión de seguridad de la inAguilera Díaz, A. (2017). El costo-beneficio como herramienta de decisión en la inversión en actividades científicas. *Cofin Habana, 11*(2), 322-343.

America Economia. (2014). *La fuga de información es una de las razones por las que las empresas pierden más dinero*. https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di

Dirección General de Modernización Administrativa. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. file:///C:/Users/Lucero/Desktop/CORE%20BUSSINES/SI/Documentos/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Fonquernie González, A. (2015, diciembre 8). *La información en las empresas*. https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/

Giesecke Sara Lafosse, M. P., & Giesecke Sara Lafosse, M. P. (2020). Elaboración y pertinencia de la matriz de consistencia cualitativa para las investigaciones en ciencias sociales. *Desde el Sur, 12*(2), 397-417. https://doi.org/10.21142/des-1202-2020-0023

Iso Tools, E. (2017). *¿Cuáles son los pasos a seguir para obtener la certificación ISO 27001?* https://www.isotools.pe/cuales-los-pasos-seguir-obtener-la-certificacion-iso-27001/

Isotools Excelence. (s. f.-a). *¿En qué consiste una matriz de riesgos?* Recuperado 9 de noviembre de 2021, de https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/

Isotools Excelence. (s. f.-b). *¿Qué es un checklist y como se debe utilizar?* Recuperado 9 de noviembre de 2021, de https://www.isotools.org/2018/03/08/que-es-un-checklist-y-como-se-debe-utilizar/

Medina León, A., Ricardo Alonso, A., Piloto Fleitas, N., Nogueira Rivera, D., Hernández Nariño, A., & Cuétara Sánchez, L. (2014). Índices integrales para el control de gestión: Consideraciones y fundamentación teórica. *Ingeniería Industrial*, *35*(1), 94-104.

NIÑO MORANTE, N. R. (2018). *MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE*. http://repositorio.unprg.edu.pe:8080/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%C3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

Norton. (2012). *13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015*. https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

OBS. (s. f.). *¿Qué es un diagrama de Gantt y para qué sirve?* OBS Business School. Recuperado 9 de noviembre de 2021, de https://www.obsbusiness.school/blog/que-es-un-diagrama-de-gantt-y-para-que-sirve

Torres Navarro, C., & Callegari Malta, N. (2016). Criterios para cuantificar costos y beneficios en proyectos de mejora de calidad. *Ingeniería Industrial, 37*(2), 151-163.

formación—Norma ISO 27001 para la fábrica Radiadores Fortaleza. *Universidad Tecnológica del Perú*. http://repositorio.utp.edu.pe/handle/20.500.12867/1933

Córdoba Perdomo, J. F. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia*. https://repositorio.upeu.edu.pe/handle/20.500.12840/4789

Gascón, M. (2021, octubre 13). *Espionaje industrial: Cuando el objetivo de los malos es infiltrarse en los recovecos cibernéticos de las empresas*. 20bits. https://www.20minutos.es/tecnologia/ciberseguridad/espionaje-industrial-cuando-el-objetivo-de-los-malos-es-infiltrarse-en-los-recovecos-ciberneticos-de-las-empresas-4852775/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la Investigación 6ta Edición*. https://librosenpdf.org/metodologia-de-la-investigacion-sampieri/

Jan, E. (s. f.). *13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015*. Recuperado 21 de octubre de 2021, de https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

JAVIER, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Llanos, S., & Elías, D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la iso/iec 27001:2013, para una empresa de consultoría de software*. 83.

Pae. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://administracionelectronica.gob.es/pae_Home#.YXdhUZ7MLIU

Torres Chango, C. D. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30690

Valdeolmillos, C. (2021, octubre 15). *Más de la mitad de empresas pierden datos por no hacer copias de seguridad suficientes*. MuyComputerPRO. https://www.muycomputerpro.com/2021/10/15/empresas-pierden-datos-copias-seguridad

Vásquez Escalante, J. F. (2018). Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. *Universidad Nacional Mayor de San Marcos*. https://cybertesis.unmsm.edu.pe/handle/20.500.12672/8436

Vilca Mosquera, E. C. (2017). Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa geosurvey de la ciudad de lima. *Universidad de Huánuco*. http://localhost:8080/xmlui/handle/123456789/809

Yagual del Valle, C., & Rodriguez, L. (2014). *Análisis para la integración de un Sistema de Gestión de Seguridad de la Información(SGSI) ISO 21002 Utilizando OSSIM para una empresa industrial*. 155.

VI. ANEXOS

VI.1. ANEXO 1. Matriz de consistencia

TITULO	FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES Y=F(X)	INDICADORES	DISEÑO DE LA INVESTIGACIÓN
"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA - 2021."	**Problema general:**	**Objetivo General:**	**Hipótesis general:**	**Variable dependiente:**	Cumplimiento de la norma ISO 27001:2013	Diseño de tipo Pre-Experimental.
	¿De qué manera la implementación del Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001:2013 permite proteger la información de los procesos Operativos en la empresa Core Business Corporation SAC ?	Implementar el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para proteger la información en los procesos Operativos en la empresa Core Business.	La implementación del Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001:2013 garantiza proteger la información de los procesos de la empresa Core Business.	La protección de información de los procesos operativos		
	Problema específico:	**Objetivos Específico:**	**Hipótesis específicas:**	**Variable independiente:**	Requisitos de la norma ISO 27001:2013	
	P1: ¿Cómo se realizará el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013? P2: ¿Cómo se realizará el diagnóstico situacional de la empresa Core Business Corporation SAC? P3: ¿ Como se elaborará el análisis de riesgo de seguridad de la información? P4: ¿Cómo se evaluará el desempeño de los colaboradores de la empresa Core Business Corporation SAC? ❖ P5: ¿Cómo se corroborará la implementación de la ISO 27001:2017 al término de la implementación?	❖ O1: Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013. ❖ O2: Elaborar el diagnóstico situacional de la empresa Core Business Corporation SAC ❖ O3: Elaborar el análisis de riesgo de seguridad de la información. ❖ O4: Evaluar el desempeño de la seguridad de información de la empresa Core Business Corporation SAC ❖O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013	❖ H1: Por medio del análisis costo-beneficio se puede determinar la viabilidad económica de la implementación de la ISO 27001:201 ❖ H2: Con el diagnóstico situacional de la empresa se identificará el cumplimiento total de la norma ISO 27001:2013. ❖ H3: Con el análisis de riesgo operacional se garantiza el cumplimiento de la norma ISO 27001:2013. ❖ H4: Evaluar el desempeño de la seguridad de información de la empresa Core Business Corporation SAC. permitirá cumplir con los objetivos de la norma ISO 27001:2013.	Norma ISO 27001:2013		

			❖H5: Asegurar el cumplimiento de la ISO 27001:2013 permite verificar el desempeño de la implementación.			

VI.2. ANEXO 2. Lista de Verificación

Figura 12

Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
4	CONTEXTO DE LA ORGANIZACIÓN		
4.1	Comprender la organización y su contexto		
4.1	La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr e(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información.	75%	Cuentan con el FOR.015 Analisis de Contexto y partes interesadas mas no especifican claramente la parte de SI
4.2	Comprender las necesidades y expectativas de las partes interesadas		
4.2	La organización debe determinar: a) las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información; y	75%	Cuentan con el FOR.015 Analisis de Contexto y partes interesadas donde se especifica a las partes interesadas como sus necesidades , espectativas y requisitos.
	b) los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.		
4.3	Determinar el alcance del sistema de gestión de seguridad de la información		
4.3	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.	75%	Cuentan con la POL.003 Alcance, mas no cuentan con una declaración de aplicabilidad de SI
	Al determinar este alcance, la organización debe considerar: a) los asuntos externos e internos tratados en 4.1		
	b) los requerimientos tratados en 4.2; y		
	c) interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.		
	El alcance estará disponible como información documentada.		La POL.003 Alcance esta en SharePoint para visualización de todos los colaboradores
4.4	Sistema de gestión de la seguridad de la información		
4.4	La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma.	75%	Cuentan con el FOR.001 Mapa de Procesos y POL.008 Caracterización de Procesos. Pero, no esta actualizado debido a nuevos cambios que se deberan hacer por los indicadores SI

Figura 12

Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
5	**LIDERAZGO**		
5.1	**Liderazgo y compromiso**		
5.1	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información al: a) asegurar que se establescan la política y los objetivos de seguridad de la información y la seguridad de la información se establezcan y sean compatibles con la dirección estratégica de la organización; b) asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información a los procesos de la organización; c) asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información están disponibles; d) comunicar la importancia de la gestión de seguridad de la información efectiva y del cumplimiento de los requisitos del sistema de gestión de la seguridad de la información; e) Asegurar que el sistema de la gestión de seguridad de la información logre su(s) resultado(s) esperado(s); f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información; g) promover la mejora continua; y h) apoyar otros roles de gestión relevantes para demostrar su liderazgo, según corresponda a sus áreas de responsabilidad.	75%	Cuentan con el FOR.002 Objetivos e indicadores, FOR.001 Mapa de Procesos, POL.008 Caracterización de Procesos mas no estan netamente relaciuonados a SI
5.2	**Política**		
5.2	La alta dirección debe establecer una política de seguridad de la información que: a) es pertinente al objetivo de la organización; b) incluya los objetivos de seguridad de la información (consulte 6.2) o que proporcione el marco de trabajo para establecer los objetivos de seguridad de la información; c) incluye un compromiso para satisfacer los requisitos aplicables, relacionados a la seguridad de la información; y d) incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información. La política de seguridad de la información debe: e) estar disponible como información documentada; f) ser comunicada dentro de la organización; y g) estar disponible para las partes interesadas, según corresponda.	25%	Si bien cuentan con POL.001 Politica de Excelencia Organizacional no cuentan con politicas SI , por ello se elaborara la Politica de dispositivos moviles, Politica de Trabajo remoto, Politica de Control de Acceso, Politica de escritorio limpio y pantalla limpia, Politica de Proveedores, Gestión de Activos entre otros que cumplen con la Aplicabilidad de SI
5.3	**Roles organizacionales, responsabilidades y autoridades**		
5.3	La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados. La alta dirección debe asignar la responsabilidad y la autoridad para: a) asegurar que el sistema de gestión de la seguridad de la información cumple con los requisitos de esta norma; y b) informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.	25%	Cuentan con el MAN.001 MOF mas no se especifican las responsabilidades respecto a SI

Figura 12

Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
6	PLANIFICACIÓN		
6.1.1	General - Acciones para abordar los riesgos y las oportunidades		
6.1.1	Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar los asuntos tratados en 4.1 y los requisitos tratados en 4.2 y determinar los riesgos y oportunidades que necesitan ser cubiertos para: a) asegurar que el sistema de gestión de la seguridad de la información pueda lograr su(s) resultado(s) esperado(s); b) evitar o disminuir efectos no deseados; y c) lograr una mejora continua. La organización debe planificar: d) acciones para abordar estos riesgos y oportunidades; y e) cómo e.1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información; y e) cómo e.2) evaluar la eficacia de estas acciones.	0%	Cuentan con el PRO.005 Gestión de riesgos y Oportunidades y FOR.013 Matriz de riesgos y oportunidades mas no cuentan con riesgos y/o oportunidades relacionadas netamente a SI
6.1.2	Evaluación de riesgo de la seguridad de la información		
6.1.2	La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información que: a) establezca y mantenga los criterios de riesgo de la seguridad de la información que incluya: a.1) los criterios de aceptación del riesgo; y a.2) los criterios para realizar las evaluaciones de riesgo de la seguridad de la información; b) asegure que las evaluaciones de riesgo de la seguridad de la información producen resultados consistentes, válidos y comparables, una y otra vez; c) identifica los riesgos de la seguridad de la información: c.1) aplica el proceso de evaluación del riesgo de la seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de la seguridad de la información; y c.2) identifica los propietarios del riesgo; d) analiza los riesgos de la seguridad de la información: d.1) evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2 c) 1) se hicieran realidad; d.2) evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y d.3) determina los niveles de riesgo; e) evalúa los riesgos de la seguridad de la información: e.1) compara los resultados del análisis de riesgo con los criterios de riesgo definidos en 6.1.2 a); y e.2) prioriza los riesgos analizados para el tratamiento de riesgo. La organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información.	0%	No se encontro evidencia, por ello se debera elaborar el procedimiento de Gestión de riesgos operacionales
6.1.3	Tratamiento de riesgo de la seguridad de la información		
6.1.3	La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para: a) seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo; b) determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida; c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido; d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A; e) formular un plan de tratamiento del riesgo de seguridad de la información; y f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual. La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.	0%	No se encontro evidencia, por ello se debera elaborar el procedimiento de Gestión de riesgos operacionales, formato de Inventario de activos y Matriz de riesgos SI
6.2	Objetivos de seguridad de la información y planificación para lograrlos		
6.2	La organización debe establecer los objetivos de seguridad de la información en niveles y funciones relevantes. Los objetivos de seguridad de la información deben: a) ser consistentes con la política de seguridad de la información; b) ser medible (si es posible); c) tomar en consideración los requisitos de seguridad de la información aplicable y los resultados de la evaluación de riesgo y el tratamiento de riesgo;	0%	Si bien cuentan con el FOR.002 Objetivos e indicadores, no se ha establecido especificamente indicadores de SI
6.2	d) ser comunicados; y e) estar actualizados según corresponda. La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información. Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar: f) qué se hará; g) qué recursos se necesitarán; h) quién será responsable; i) cuándo se terminará; y j) cómo se evaluarán los resultados.	0%	Si bien cuentan con e FOR.002 Objetivos e indicadores FOR.033 Programa anual de comunicación y sensibilización POL.007 Plan de Comunicación No se ha establecido especificamente comunicados de SI

Figura 12

Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
7	**APOYO**		
7.1	**Recursos**		
7.1	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.	0%	Se cuenta con el FOR.032 Organigrama y MAN.001 MOF, mas no se es especifica con SI
7.2	**Competencias**		
7.2	La organización debe: a) determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño de seguridad de la información; b) asegurar que estas personas sean competentes basados en una educación, capacitación o experiencia adecuada; c) cuando corresponda, tomar las acciones para adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas; y d) retener la información documentada adecuada como evidencia de competencia.	25%	Se cuenta con el FOR.016 Plan anual de capacitaciones, pero falta actualizarlo relacionandolo a SI
7.3	**Conocimiento/Concientización**		
7.3	Las personas que trabajen bajo el control de la organización deben estar al tanto de: a) la política de seguridad de la información; b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios del desempeño mejorado de la seguridad de la información; y c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.	25%	Inducción y FOR.033 Programa anual de comunicación y sensibilización, pero se debe actualizar para brindar todo lo relacionado a SI
7.4	**Comunicación**		
7.4	La organización debe determinar la necesidad de comunicaciones internas y externas que sean pertinentes al sistema de gestión de seguridad de la información que incluya: a) qué comunicar; b) cuándo comunicarlo; c) con quién comunicarlo; d) quién debe comunicarlo; y e) los procesos que se verán afectados por la comunicación.	25%	FOR.033 Programa anual de comunicación y sensibilización
7.5.1	**Información documentada**		
7.5.1	El sistema de gestión de la seguridad de la información debe incluir: a) información documentada necesaria para esta norma; y b) información documentada, definida por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.	25%	PRO.001 Control de información documentada
7.5.2	**Creación y actualización**		
7.5.2	Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente: a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia); b) formato (por ejemplo, idioma, versión de software, gráficos) y medio (por ejemplo, papel, digital); y c) revisión y aprobación para conveniencia y suficiencia.	25%	PRO.001 Control de información documentada
7.5.3	**Control de la información documentada**		
7.5.3	La información documentada necesaria por el sistema de gestión de la seguridad de la información y por la norma debe ser controlada para asegurar que: a) está disponible y apropiada para su uso, donde y cuando sea necesario; y b) está debidamente protegida (por ejemplo, de pérdidas de confidencialidad, uso inapropiado o pérdida de integridad). Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda: c) distribución, acceso, recuperación y uso; d) almacenamiento y conservación, incluida la conservación de la legibilidad; e) control de cambios (por ejemplo, control de versión); y f) retención y disposición. Información documentada de origen externo, determinada por la organización, de ser necesario, para la planificación y operación del sistema de gestión de la seguridad de la información debe ser identificado como apropiado y controlado.	75%	Cuentan con el PRO.001 Control de información documentada

Figura 12

Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
8	OPERACIÓN		
8.1	Control y planificación operacional		
8.1	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en 6.1. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información, definidos en 6.2.	0%	
	La organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado.		
	La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario. La organización se debe asegurar de que los procesos externalizados se determinan y controlan.		
8.2	Evaluación de riesgo de la seguridad de la información		
8.2	La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos, considerando los criterios establecidos en 6.1.2 a).	0%	No se cuenta con evidencia de una evaluación de riesgo de la seguridad de la información
	La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.		
8.3	Tratamiento de riesgo de la seguridad de la información		
8.3	La organización debe implementar el plan de tratamiento del riesgo de la seguridad de la información.	50%	Se cuenta con el PRO.002 tratamiento de NC y AC
	La organización debe conservar la información documentada de los resultados del tratamiento del riesgo de la seguridad de la información.		
9	EVALUACIÓN DEL DESEMPEÑO		
9.1	Monitoreo, medición, análisis y evaluación		
9.1	La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la seguridad de la información. La organización debe determinar: a) qué se necesita monitorear y medir, incluidos los controles y procesos de la seguridad de la información;	25%	Se cuenta con un FOR.002 Objetivos de SIG, mas no especifica los objetivos de SI
	b) los métodos para monitorear, medir, analizar y evaluar, según corresponda, para asegurar resultados válidos;		
	c) cuándo se deben llevar a cabo el monitoreo y la medición;		
	d) quién debe monitorear y medir;		
	e) cuándo se deben analizar y evaluar los resultados del monitoreo y la medición; y		
	f) quién debe analizar y evaluar estos resultados.		
	La organización debe conservar la información documentada correspondiente, como evidencia de los resultados del monitoreo y medición.		
9.2	Auditoría Interna		
9.2	La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información:	75%	Se cuenta con el PRO.003 Gestió de Auditorias
	a) cumple con:		
	a.1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y		
	a.2) los requisitos de esta norma;		
	b) está debidamente implementada y mantenida. La organización debe:		
	c) planificar, establecer, implementar y mantener programa(s) de auditoría, incluida la frecuencia, métodos, responsabilidades, requisitos de planificación e informes. El (los) programa(s) de auditoría debe(n) considerar la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;		
	d) definir los criterios de auditoría y el alcance para cada auditoría;		
	e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;		
	f) asegurar que los resultados de las auditorías son informados a la dirección pertinente; y		
	g) conservar la información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.		
9.3	Revisión de gestión		
9.3	La alta dirección debe revisar el sistema de gestión de la seguridad de la información en los plazos planificados para asegurar su conveniencia, suficiencia y efectividad continua. La revisión de la dirección debe considerar: a) el estado de las acciones, a partir de las revisiones de gestión anteriores;	75%	Se cuenta con el PRO.007 Revisión por la Dirección
9.3	b) los cambios en los asuntos externos e internos que son pertinentes al sistema de gestión de la seguridad de la información;		
	c) los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en: 1) no conformidades y acciones correctivas;		
	2) resultados del monitoreo y mediciones;		
	3) resultados de auditoría; y		
	4) cumplimiento de los objetivos de seguridad de la información;		
	d) comentarios de las partes interesadas;		
	e) resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo; y		
	f) las oportunidades para la mejora continua.		
	Los resultados de la revisión de dirección deben incluir las decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambios al sistema de gestión riesgo; y		
	La organización debe conservar la información documentada como evidencia de los resultados de las revisiones de gestión.		

Figura 12

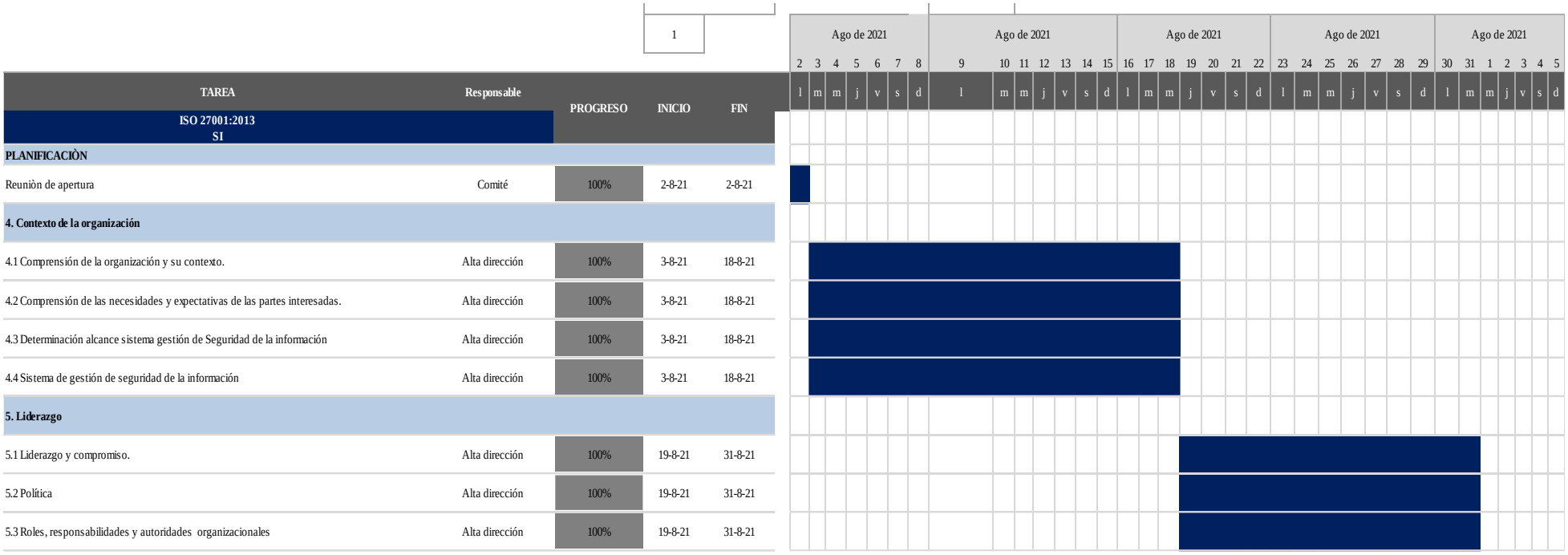
Lista de Verificación

CLAUSULA	Requisito obligatorio para el SGSI	Estado(Evaluación)	Evidencia de cumplimiento
10	**MEJORA**		
10.1	**No Conformidades y acciones correctivas**		
10.1	Cuando ocurre una no conformidad, la organización debe: a) reaccionar frente a la no conformidad y si corresponde: a.1) tomar acciones para controlarlo y corregirlo; y	50%	Se cuenta con el PRO.002 Tratamiento de NC y AC
	a.2) encargarse de las consecuencias;		
	b) evaluar la necesidad de acción para eliminar las causas de no conformidad, y que así esto no vuelva a ocurrir o que ocurra en otro lugar, al: 1) revisar la no conformidad;		
	2) determinar las causas de las no conformidades; y		
	3) determinar si existe una no conformidad similar o podría ocurrir;		
	c) implementar cualquier acción necesaria;		
	d) revisar la efectividad de cualquier acción correctiva implementada; y		
	e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.		
	Las acciones correctivas deben ser pertinentes a los efectos de las no conformidades halladas.		
	La organización debe conservar la información documentada como evidencia de: f) la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y		
	g) los resultados de cualquier acción correctiva.		
10.2	**Mejora continua**		
10.2	La organización debe mejorar de manera continua la conveniencia, suficiencia y efectividad del sistema de gestión de la seguridad de la información.	50%	Se cuenta con el PRO.002 Tratamiento de NC y AC

VI.3. ANEXO 3. Diagrama Gantt

Figura 13

Diagrama de Gantt

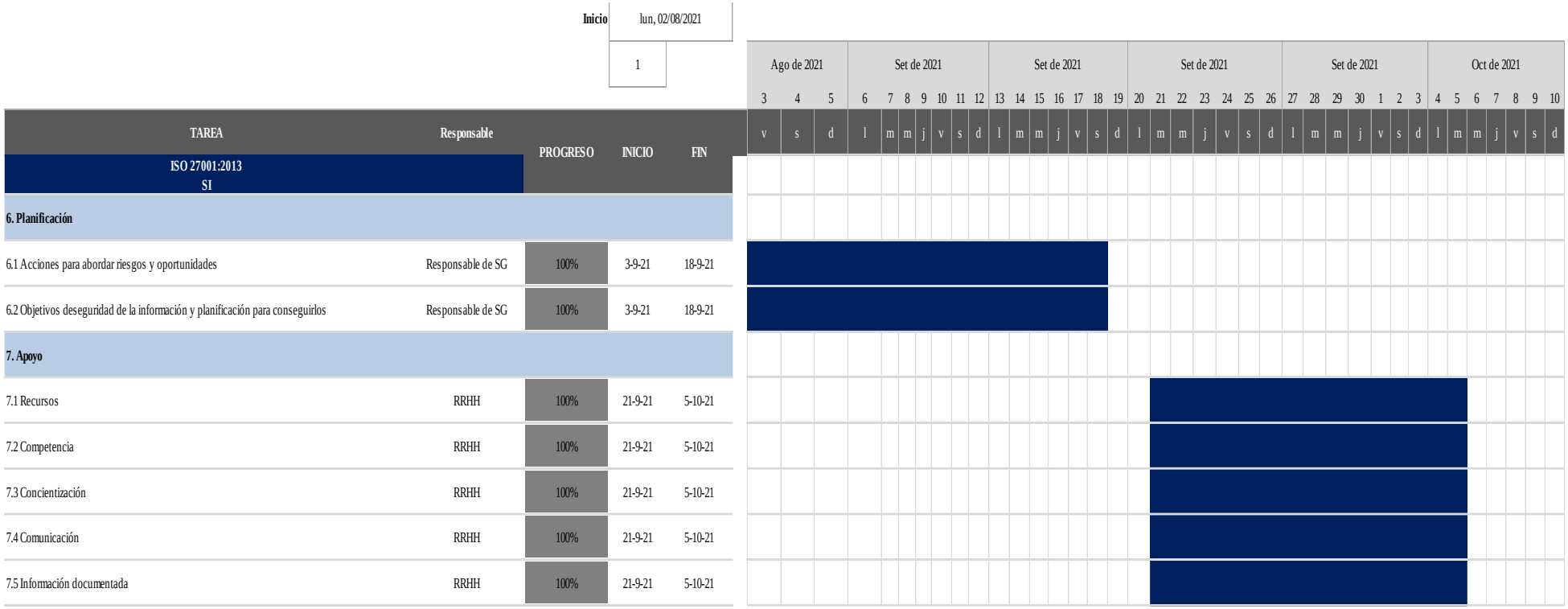


TAREA	Responsable	PROGRESO	INICIO	FIN
ISO 27001:2013 SI				
PLANIFICACIÒN				
Reuniòn de apertura	Comité	100%	2-8-21	2-8-21
4. Contexto de la organización				
4.1 Comprensión de la organización y su contexto.	Alta dirección	100%	3-8-21	18-8-21
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.	Alta dirección	100%	3-8-21	18-8-21
4.3 Determinación alcance sistema gestión de Seguridad de la información	Alta dirección	100%	3-8-21	18-8-21
4.4 Sistema de gestión de seguridad de la información	Alta dirección	100%	3-8-21	18-8-21
5. Liderazgo				
5.1 Liderazgo y compromiso.	Alta dirección	100%	19-8-21	31-8-21
5.2 Política	Alta dirección	100%	19-8-21	31-8-21
5.3 Roles, responsabilidades y autoridades organizacionales	Alta dirección	100%	19-8-21	31-8-21

VI.4. ANEXO 3. Diagrama Gantt

Figura 13

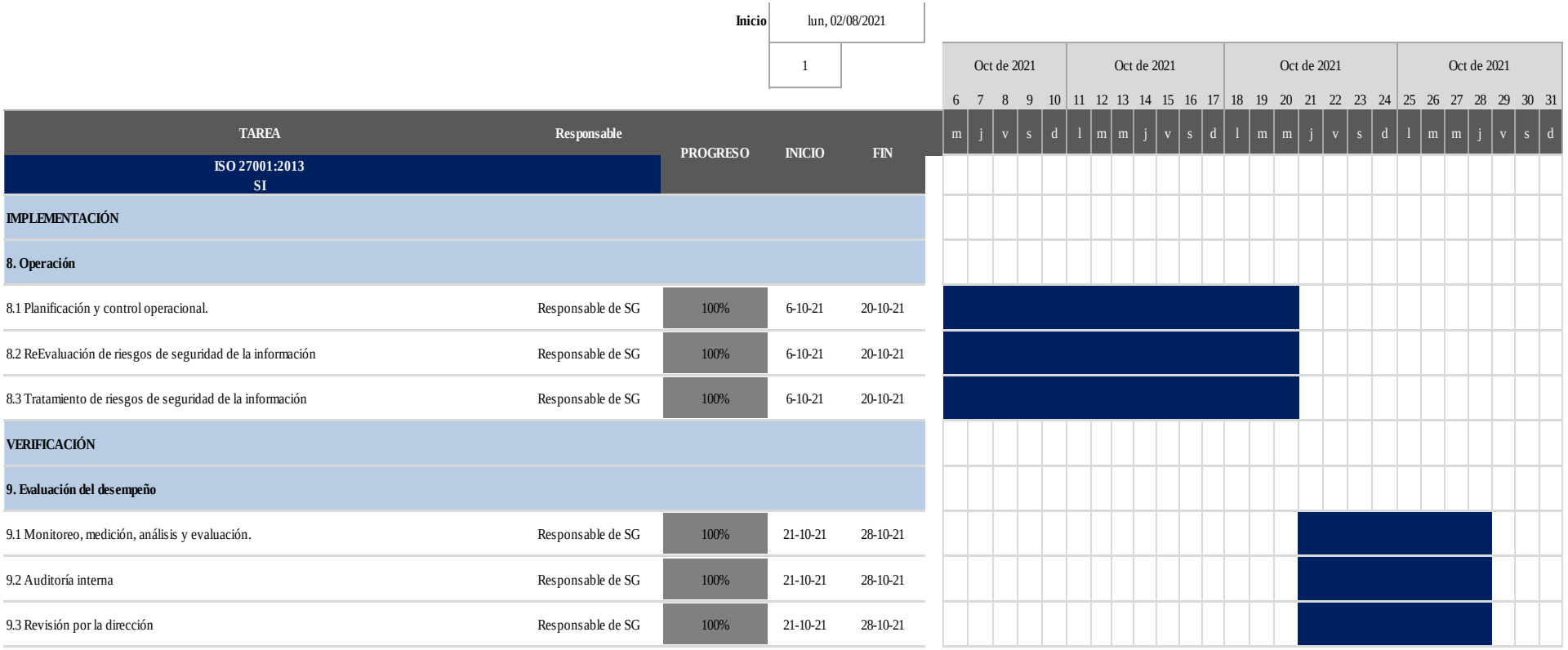
Diagrama de Gantt



VI.5. ANEXO 3. Diagrama Gantt

Figura 13

Diagrama de Gantt



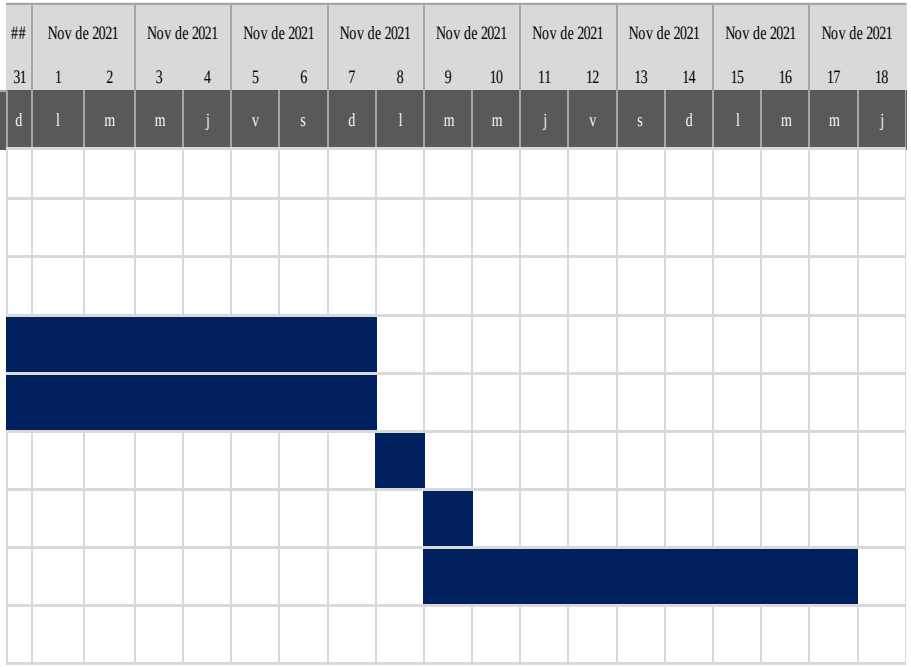
Inicio	lun, 02/08/2021
	1

TAREA ISO 27001:2013 SI	Responsable	PROGRESO	INICIO	FIN
IMPLEMENTACIÓN				
8. Operación				
8.1 Planificación y control operacional.	Responsable de SG	100%	6-10-21	20-10-21
8.2 ReEvaluación de riesgos de seguridad de la información	Responsable de SG	100%	6-10-21	20-10-21
8.3 Tratamiento de riesgos de seguridad de la información	Responsable de SG	100%	6-10-21	20-10-21
VERIFICACIÓN				
9. Evaluación del desempeño				
9.1 Monitoreo, medición, análisis y evaluación.	Responsable de SG	100%	21-10-21	28-10-21
9.2 Auditoría interna	Responsable de SG	100%	21-10-21	28-10-21
9.3 Revisión por la dirección	Responsable de SG	100%	21-10-21	28-10-21

Figura 13

Diagrama de Gantt

TAREA	Responsable	PROGRESO	INICIO	FIN
ISO 27001:2013 SI				
ACTUAR				
10. Mejora				
10.1 No conformidades y acciones correctivas.	Responsable de SG	100%	31-10-21	7-11-21
10.2 Mejora continua.	Responsable de SG	100%	31-10-21	7-11-21
Reunión de cierre de implementación	Responsable de SG	100%	8-11-21	8-11-21
Culminacion de la implementacion ISO 27001:2013	Responsable de SG	100%	9-11-21	**9-11-21**
Verificación de Cumplimiento de controles	Responsable de SG	100%	9-11-21	**24-11-21**
Verificación de Cumplimiento de la ISO 27001:2013	Responsable de SG	200%	24-11-21	**26-11-21**



VI.6. ANEXO 4. Lista de verificación de expertos

Figura 14

Lista de verificación de expertos

Título de la investigación:	"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA - 2021."
Línea de investigación:	Desarrollo sostenible y Gestión empresarial
Apellidos y nombres del experto:	VELASQUEZ ALIAGA DANTE YHANCARLO
El instrumento de medición pertenece a la variable:	Lista de verificación

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

DNI: 43159894
CIP: 191332

Figura 14

Lista de verificación de expertos

Título de la investigación:	"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA – 2021."
Línea de investigación:	Desarrollo sostenible y Gestión empresarial
Apellidos y nombres del experto:	Da Cruz Rodriguez Abby Solange
El instrumento de medición pertenece a la variable:	Lista de verificación

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Ítems	Preguntas	Aprecia		Observaciones
		SI	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	x		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	x		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	x		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	x		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	x		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	x		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	x		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	x		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	x		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	x		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	x		

Sugerencias:

Firma del experto:

DNI: 71612630
CIP: 168766

Figura 14

Lista de verificación de expertos

Título de la investigación:	"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA - 2021."
Línea de investigación:	Desarrollo sostenible y Gestión empresarial
Apellidos y nombres del experto:	ALIAGA MORI CELESTINO PAUL
El instrumento de medición pertenece a la variable:	Lista de verificación

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

DNI: 47511500
CIP: 191040

VI.7. ANEXO 5. Lista maestra

Figura 15

Lista maestra

MACROPROCESO	SUB PROCESO	TIPO	CODIGO	NOMBRE	INTERNO (I)/ EXTERNO (E)	ESTADO
_02_Procesos_Operativos	01 - Gestión comercial	Procedimiento	PRO.018	Gestión Comercial	Interno	VIGENTE
_02_Procesos_Operativos	01 - Gestión comercial	Formato	FOR.037	Lista de Requisitos del Servicio	Interno	VIGENTE
_02_Procesos_Operativos	01 - Gestión comercial	Formato	FOR.045	Evaluación del Servicio del Cliente	Interno	VIGENTE
_02_Procesos_Operativos	01 - Gestión comercial	Formato	FOR.046	Requerimiento del Servicio	Interno	VIGENTE
_02_Procesos_Operativos	01 - Gestión comercial	Formato	FOR.056	Evaluación de Seguimiento de Proyectos	Interno	VIGENTE
_02_Procesos_Operativos	02 - Visitas Técnicas	Procedimiento	PRO.016	Auditoria , Inspeccion y Asesoría	Interno	VIGENTE
_02_Procesos_Operativos	02 - Visitas Técnicas	Formato	FOR.047	Requerimiento de Auditoria	Interno	VIGENTE
_02_Procesos_Operativos	02 - Visitas Técnicas	Formato	FOR.040	Planeación del servicio	Interno	VIGENTE
_02_Procesos_Operativos	02 - Visitas Técnicas	Formato	FOR.038	Equipos de protección personal	Interno	EN REVISIÓN
_02_Procesos_Operativos	04 - Capacitación	Procedimiento	PRO.012	Servicio de Capacitaciones a Clientes Externos	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.060	Listado de Capacitaciones	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.022	Requerimiento de Capacitación	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.059	Requerimiento Plataforma E-corelearning	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.023	Formato de Silabo	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.024	Modelo de certificado / constancia.	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Manual	MAN.003	Manual de usuario de la plataforma.	Interno	EN REVISIÓN
_02_Procesos_Operativos	04 - Capacitación	Política	POL.004	Lineamientos Operacionales para el Servicio de Capacitaciones al cliente externo	Interno	VIGENTE
_02_Procesos_Operativos	04 - Capacitación	Formato	FOR.061	Requerimiento de Certificados/constancias	Interno	VIGENTE
MACROPROCESO	SUB PROCESO	TIPO	CODIGO	NOMBRE	INTERNO (I)/ EXTERNO (E)	ESTADO
_01_Estratégico	02 - Plan Estratégico	Formato	FOR.032	Organigrama	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Instructivo	INS.001	Elaboración de Planificación Estratégica	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Formato	POL.002	Planificación Estratégica de CBC	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Procedimiento	PRO.007	Revision por la dirección	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Política	POL.003	Alcance del SIG	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Formato	FOR.015	Análsis de Contexto y partes interesadas	Interno	VIGENTE
_01_Estratégico	02 - Plan Estratégico	Política	POL.009	Rendición de Cuentas	Interno	VIGENTE

Figura 15

Lista maestra

MACROPROCESO	SUB PROCESO	TIPO	CODIGO	NOMBRE	INTERNO (I)/ EXTERNO (E)	ESTADO
_01_Estratégico	01 - SIG	Política	POL.001	Política de Excelencia Organizacional	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.001	Mapa de procesos	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.002	Objetivos e indicadores del SIG	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.003	Programa Anual SIG	interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.004	Acta de Comité	Interno	VIGENTE
_01_Estratégico	01 - SIG	Manual	MAN.002	Manual del Sistema Integrado de Gestión	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.001	Control de Información Documentada	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.005	Lista Maestra de Información Documentada	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.002	Tratamiento de No conformidad y Acción Correctiva	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.006	Registro de Acciones correctivas	Interno	ELIMINADO
_01_Estratégico	01 - SIG	Formato	FOR.007	Base de datos de acciones corretivas	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.008	Lista de Servicios y no conformidades	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.003	Gestión de Auditoria	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.009	Programa Anual de Auditorías	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.010	Plan de Auditoria	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.011	Informe de auditoría interna	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.004	Gestión del Cambio	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.012	Solicitud de Gestión del Cambio	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.005	Gestión del Riesgo y Oportunidades	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.013	Matriz de gestión de riesgos y oportunidades	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.006	Medicion de satifacción al Cliente	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.053	Base de Datos de Encuestas de Satisfacción	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.029	Encuesta Satisfacción de Capacitaciones	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.030	Encuesta Satisfacción de Auditoría/Inspección	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.031	Encuesta Satisfacción de Asesoría	Interno	VIGENTE
_01_Estratégico	01 - SIG	Formato	FOR.058	Encuesta Satisfacción de Plataforma de capacitación	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.019	Gestión de emergencias	Interno	EN REVISIÓN
_01_Estratégico	01 - SIG	Procedimiento	PRO.020	IPERC	Interno	EN REVISIÓN
_01_Estratégico	01 - SIG	Formato	FOR.042	Matriz IPERC	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	PRO.021	Requisitos Legales	Interno	VIGENTE
_01_Estratégico	01 - SIG	Procedimiento	FOR.041	Matriz de Requisitos Legales y Otros	Interno	VIGENTE
01_Estratégico	01 - SIG	Política	POL.008	Caracterización del proceso	Interno	VIGENTE

Figura 15

Lista maestra

MACROPROCESO	SUB PROCESO	TIPO	CODIGO	NOMBRE	INTERNO (I)/ EXTERNO (E)	ESTADO
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Procedimiento	PRO.008	Capacitación	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.016	Plan Anual de Capacitaciones Internas	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.017	Carta de Compromiso	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Política	POL.007	Política Plan de Comunicaciones	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.033	Programa de comunicaciones y sencibilización	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.054	Programa de Investigaciones	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Manual	MAN.001	Manual de Organización y Funciones	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Procedimiento	PRO.009	Gestión de RR.HH.	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Procedimiento	PRO.010	Sistema de Desarrollo Profesional	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.018	Evaluación del Desempeño	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Política	POL.005	Codigo de Vestimenta	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.049	Confidencialidad del Personal	Interno	VIGENTE
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.055	Formato de Inducción	Interno	VIGENTE
_03_Procesos_Apoyo	02 - Gestión de Proveedores	Procedimiento	PRO.011	Gestión de Proveedores	Interno	VIGENTE
_03_Procesos_Apoyo	02 - Gestión de Proveedores	Formato	FOR.019	Plantilla de Evaluación	Interno	VIGENTE
_03_Procesos_Apoyo	02 - Gestión de Proveedores	Formato	FOR.020	Lista de proveedores autorizados	Interno	VIGENTE
_03_Procesos_Apoyo	02 - Gestión de Proveedores	Formato	FOR.021	Acuerdo de Servicio	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Política	POL.006	Política de Gastos de Viajes	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.025	Solicitud de Boleto Aéreo	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.026	Solicitud de AGV	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.027	Rendición de Viáticos	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.028	Movilidad	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Procedimiento	PRO.013	Rendición de Gastos	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Instructivo	INS.002	Instructivo de Emisión y Envío de Facturas	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Procedimiento	PRO.014	Facturación	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.014	Formato de Sustento de Gastos	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.039	Matriz de Bienes de SST	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Formato	FOR.050	Acta de Entrega de Bienes	Interno	VIGENTE
_03_Procesos_Apoyo	04 - Gestión de Recursos Financieros	Procedimiento	PRO.017	Compras de Bienes	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.003	Creación de nuevo correo en CPANEL	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.004	Backup de Correo	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.005	Mantenimiento preventivo de Equipos de computo	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.006	Compartir información - Sharepoint	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	PRO.015	Infraestructura tecnológica	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.007	Backup de información de SharePoint	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.008	Eliminación de correo	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.036	Compromiso de seguridad de la información	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.010	Mantenimiento buzo de correos en el servidor	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Instructivo	INS.011	Configuración y backup de correo en equipo	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.034	Formato préstamo de laptop	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.035	Formato de informacion del personal nuevo y entrega de equipos	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.043	Registro de Backup de Información	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.057	Programa de Soporte informático	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.044	Registro de Licencias	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	POL.010	Protocolo para Reuniones Virtuales	Interno	VIGENTE
_03_Procesos_Apoyo	05 - SST	Procedimiento	PRO.022	Comunicación, Participación y Consulta.	Interno	VIGENTE
_03_Procesos_Apoyo	06 - SI	Política	POL.011	Política dispositivos moviles	Interno	
_03_Procesos_Apoyo	06 - SI	Política	POL.012	Política de trabajo remoto	Interno	
_03_Procesos_Apoyo	06 - SI	Política	POL.013	Política de control de acceso	Interno	
_03_Procesos_Apoyo	06 - SI	Política	POL.014	Política de escritorio limpio y pantalla limpia	Interno	
_03_Procesos_Apoyo	06 - SI	Política	POL.015	Política de proveedores	Interno	
_03_Procesos_Apoyo	01 - Gestión de RR.HH.	Formato	FOR.052	Lista de asistencia de capacitacion	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.062	Inventario de Activos	Interno	VIGENTE
_03_Procesos_Apoyo	03 - Infraestructura	Formato	FOR.063	Matriz de riesgos SI	Interno	VIGENTE
_03_Procesos_Apoyo	06 - SI	Política	POL.016	Gestión de Activos	Interno	
_03_Procesos_Apoyo	06 - SI	Política	POL.017	Uso aceptable de los activo	Interno	
_03_Procesos_Apoyo	06 - SI	Procedimiento	PRO.023	Gestión de riesgos Operacionales	Interno	VIGENTE
_03_Procesos_Apoyo	06 - SI	Procedimiento	PRO.024	Gestión de Incidentes Seguridad de Información	Interno	VIGENTE

VI.8. ANEXO 6. Aplicabilidad

Figura 16

Aplicabilidad

	FORMATO	Código: FOR.064	
Core Business	APLICABILIDAD	Fecha de publicación:	Versión:
		8/10/2021	1

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
5.1 Política de seguridad de la información	5.1.1 Políticas de seguridad de la información	SI	Es de vital importancia que exista un conjunto de políticas que permitan asegurar la información y que pueda ser comunicado a todo los colaboradores y partes interesadas pertinentes.	Todas las Políticas de Seguridad de la Información
	5.1.2 Revisión de las políticas de seguridad de la información	SI	Periódicamente se debe realizar la revisión de las políticas integradas con la finalidad de garantizar la eficacia de las mismas.	Todas las Políticas de Seguridad de la Información especifican con que frecuencia se revisa
6.1 Organización Interna	6.1.1 Roles y responsabilidades de la seguridad de la información	SI	Se debe gestionar la seguridad de la información definiendo responsabilidades por parte de la gerencia.	*En el MAN.001 Manual de Organización y Funciones evidencia la responsabilidad general que todos los colaboradores. *Las responsabilidades para cada activo se encuentra en la PRO.025 Gestión de activos *Los propietarios de los activos y los custodios se encuentran en el FOR.062 Inventario de activos.
	6.1.2 Segregación de funciones	SI	Es necesario que se lleve a cabo la gestión de la seguridad en base a las competencias por areas que posee CBC y asignar un personal adecuado.	MAN.001 Manual de Organización y Funciones
	6.1.3 Contacto con autoridades	SI	Periódicamente se debe mantener contacto con el Oficial de SI ya que el gestionaran la seguridad de la información con el fin de monitoriar y regular los procesos para que se lleven a cabo.	FOR.064 Lista de Contactos
	6.1.4 Contacto con grupos especiales de interés	SI	Se debe compartir información con grupos de interés para tener mejor tratamiento del riesgo en cuanto a la seguridad de la información.	Lista de Contactos
	6.1.5 Seguridad de la informacion en la gestion de proyectos	SI	Se debe identificar y tratar los riesgos de la información y los requisitos de seguridad en todas las fases de los proyectos. Esto se aplica en general a cualquier proyecto, independientemente de su carácter, por ejemplo, un proyecto para un proceso clave de negocio, de TI, de gestión de instalaciones y otros procesos de apoyo	PRO.023 Gestión de riesgos operacionales FOR.063 Matriz de riesgos SI
6.2 Dispositivos móviles y trabajo remoto	6.2.1 Política de dispositivos móviles	SI	Se debe definir controles y pautas respecto al uso que se le den a los dispositivos moviles	POL.011 Politica de dispositivos moviles
	6.2.2 Trabajo remoto	SI	Es necesario definir controles y pautas respecto al trabajo remoto que se realiza en un ámbito diferente a la oficina. Se debería implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada por los colaboradores.	POL.012 Politica de trabajo remoto
7.1 Antes del empleo	7.1.1 selección	SI	Es necesario que se investigue los antecedentes penales al aspirante en el proceso de reclutamiento para evitar inconvenientes a futuro.	PRO.009 Gestion de RRHH
	7.1.2 Términos y condiciones de la relación laboral	SI	En el proceso de contratación se debe dar a conocer las normativas y políticas que el colaborador deberá acatar.	Contratos de Trabajo / FOR.035 Compromiso de Seguridad de la Información
7.2 Durante el empleo	7.2.1 Responsabilidad de la Gerencia	SI	Debe existir un programa de sensibilización sobre la seguridad de la información dirigido por la gerencia para el conocimiento y la capacitación apropiada a todos los colaboradores de CBC	FOR.033 Programa de comunicacion y sensibilizacion MAN.001 MOF
	7.2.2 Concientización, educación y formacion en seguridad de la informacion	SI	Es necesario un programa de sensibilización y capacitación sobre seguridad de la información que involucre a todos los colaboradores de CBC.	FOR.033 Programa de comunicacion y sensibilizacion PRO.008 Plan de Capacitación Interna
	7.2.3 Proceso disciplinario	SI	Se debe explicar al nuevo colaborador el proceso de disciplina que debe cumplir para evitar incumplimiento a la privacidad, mal uso de la información,fraude y acceso no autorizado	PRO.009 Gestión de RRHH / Proceso Disciplinario
7.3 Terminacion y cambio de empleo	7.3.1 Responsabilidades en la desvinculación o cambio de empleo	SI	Antes del contrato es importante mencionar las políticas sobre el derecho que se le otorga al cese o cambio del lugar de trabajo con la finalidad de que a futuro no existan inconvenientes.	Contratos PRO.009 Gestión de RRHH / Procedimiento de Terminación de Relación Laboral FOR.035 Compromiso de Seguridad de la Información

Figura 16

Aplicabilidad

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
6.2 Dispositivos móviles y trabajo remoto	6.2.1 Política de dispositivos móviles	SI	Se debe definir controles y pautas respecto al uso que se le den a los dispositivos moviles	POL.011 Politica de dispositivos moviles
8.1Gestion de activos	8.1.1 Inventario de activos	SI	Todos los activos deben estar identificados y mantenerlo actualizado.	POL.016 Gestión de ctivos FOR.062 Inventario de Activos
	8.1.2 Propiedad de los activos	SI	El propietario del activo debería ser responsable de la adecuada gestión del activo durante todo su ciclo de vida. CBC cuenta con el Oficial de información quien tiene a su cargo la responsabilidad de los activos de información por lo que debe llevar un control adecuado de los mismos. Pero, las tareas rutinarias pueden delegarse, por ejemplo, a un custodio al cuidado diario de los activos.	POL.016 Gestión de ctivos FOR.062 Inventario de Activos
	8.1.3 Uso aceptable de los activos	SI	Es importante la existencia de los controles sobre los activos para el correcto uso de los recursos y por ende de la información.	En la POL.017 Política de uso aceptable de los activos en la que se establecen el uso que los colaboradores le deben dar a los activos
	8.1.4 Retorno(Devolución) de los activos	SI	Debe existir un procedimiento automatizado para recuperar los activos tras una baja o despido y así garantizar que estos no sean manipulados de manera incorrecta.	PRO.009/Procedimiento de Terminación de Relación Laboral(Gestion RRHH-formato de devolucion) POL.016 Gestión de Activos
8.2 Clasificación de la información	8.2.1 Clasificación de la informacion	SI	Es importante contar con políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información obteniendo los requisitos de confidencialidad, integridad y disponibilidad con conocimiento a todos los colaboradores.	POL.016 Gestión de activos
	8.2.2 Etiquetado de la informacion	SI	Mediante el proceso de etiquetado para la información física debe estar sincronizado a la clasificación de la información.	POL.016 Gestión de activos
	8.2.3 Manejo de activos	SI	Se debe establecer medidas de control que verifiquen que solo el personal autorizado pueda manipular la información de los activos.	POL.016 Gestión de activos
8.3 Manejo de los medios	8.3.1 Gestión de los medios removibles	SI	Se debe contar con controles apropiados para el registro de medios removibles, etiquetados y clasificados de forma adecuada para mantener la confidencialidad de los datos almacenados.	POL.016 Gestión de activos
	8.3.2 Disposicion(Eliminación) de los medios	SI	El proceso de eliminación de soporte debe estar ligado a quien autorice el acto, documentando la aprobación del mismo.	POL.016 Gestión de activos
	8.3.3 Transferencia física de los medios fisicos	SI	Es de necesario cumplir con los controles se seguridad para que el transporte o el servicio de mensajería sean confiables.	POL.016 Gestión de activos
9.1 Requisito de la empresa para el control de acceso	9.1.1 Política de control de acceso	SI	Es necesario tener las políticas de control de acceso documentado y aprobado por el que gestiona la información	POL.013 Politica de control de acceso
	9.1.2 Acceso a las redes y a los servicios de la red	NO	La seguridad en el acceso VPN debe ser supervisado, controlados y autorizados para evitar el hurto de información.	Paul: Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre
9.2 Gestión de acceso de los usuarios	9.2.1 Registro y baja(cancelación) de registros de usuarios	SI	Es importante que los usuarios tengas un ID único para facilidad de gestionar cualquier acontecimiento y se pueda resolver de manera adecuada.	Paul: Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre
	9.2.2 Aprovisionamiento(Asignación) de acceso de usuario	SI	El control de acceso a los usuarios debe garantizar que se concede de acuerdo a las políticas de control de acceso y segregación de las funciones.	Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre /POLITICAS
	9.2.3 Gestión de derechos de acceso privilegiados	SI	Debe existir un proceso para realizar revisiones más frecuentes y periódicas de las cuentas privilegiadas con el fin de monitorizar actividades ejecutadas.	Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre /POLITICAS
	9.2.4 Gestión de información secreta de autenticación de usuarios	SI	Se debe gestionar correctamente controles técnicos para la identidad de los usuarios.	
	9.2.5 Revisión de los derechos de acceso de usuarios	SI	Debe existir una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones.	Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre /POLITICAS
	9.2.6 Remocion(Eliminación) o ajuste de los derechos de acceso	SI	Debe tomarse como medidas de prevención, los retiros de privilegios en acceso de información y contraseñas a los usuarios que se le sea terminado el contrato.	Analicemos si puede ir en un procedimiento de Tecnologia o TI, busquemos el nombre /POLITICAS

Figura 16

Aplicabilidad

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
6.2 Dispositivos móviles y trabajo remoto	6.2.1 Política de dispositivos móviles	SI	Se debe definir controles y pautas respecto al uso que se le den a los dispositivos moviles	POL.011 Politica de dispositivos moviles
9.3 responsabilidad de los usuarios	9.3.1 Uso de información de autenticación secreta	SI	Es necesario que exista un factor de aseguramiento de la confidencialidad de las credenciales de autentificación	FOR.035 Compromiso de Seguridad de la Información
9.4 Control de acceso al sistema y aplicación	9.4.1 Restricción de acceso a la información	SI	Debe existir accesos adecuados para el control de usuarios de forma individual para restringir a personas ajenas a la empresa.	Controles de acceso físico (seguridad física) Controles de acceso a los sistemas de informacion
	9.4.2 Procedimiento de inicio de sesión seguro	SI	Debe existir una pantalla de advertencia de inicio de sesión para disuadir el acceso no autorizado	Control de acceso a los sistemas (Usuario y contraseña)
	9.4.3 Sistema de gestión de contraseñas	SI	Los sistemas deben requerir que las contraseñas se establezcan bajo políticas y estándares corporativos de manera que se almacenen de forma segura (cifrada).	POL.013 Politica de control de acceso
	9.4.4 Uso de programas utilitarios privilegiados	SI	Debe existir una persona encargada que controle los servicios privilegiados bajo condiciones con verificación de acuerdo a sus roles y responsabilidades.	Declaración de cuentas privilegiadas
	9.4.5 Control de acceso al código fuente de los programas	NO	El almacenamiento del código fuente debe mantenerse en un controlador de versiones de forma segura para un monitoreo consecuente de quien realice diferentes actividades dentro de ella.	
10.1 Controles criptográficos	10.1.1 Política sobre el uso de controles criptográficos	NO	Debe existir una política que cubra el uso de controles criptográficos, así como la información debe ser protegida a través de la criptografía. Uso de cifrado para información almacenada o transferida.	Politica/cada vez que se quiera comparti información controles criptografcios(recomendacioens)
	10.1.2 Gestión de claves	NO	Proteger el equipo utilizado para generar, almacenar y archivar claves.	
11.1 seguridad fisica y ambiental	11.1.1 Perímetro de seguridad física	NO	Se deben establecer perímetros de seguridad para proteger aquellas áreas con equipamiento importante o con instalaciones donde se procesa información En el caso de CBC cuenta con un trabajo remoto	Centros de Datos / Instalaciones / Perímetros de seguridad física
	11.1.2 Controles de ingreso(acceso) físico	NO	Para evitar mal uso del equipamiento es importante que se definan controles de entrada para asegurar el acceso de solo personal autorizado. CBC cuenta con un trabajo remoto	Personal de vigilancia/camaras
	11.1.3 Seguridad de oficinas, salas e instalaciones	NO	Debe existir procedimientos para mantener la confidencialidad e integridad en las diferentes áreas. CBC cuenta con un trabajo remoto	
	11.1.4 Protección contra amenazas externas y del ambiente	NO	Debe existir un plan de gestión de riesgos ante eventualidades externas como sismos, incendios,ataques , para evitar el daño de equipos y mucho menos la pérdida de información.	Centros de Datos / Instalaciones / Controles de seguridad contra amenazas externas y del ambiente Plan de contingencia Capacitación
	11.1.5 Trabajo en áreas seguras	NO	Se debe realizar verificaciones en los puestos de trabajos y tener en cuenta que no pueden utilizar cualquier mecanismo de grabación	Centros de Datos / Instalaciones / Perímetros de seguridad física
	11.1.6 Áreas de entrega y carga	NO	No existe un procedimientos para la carga y descarga de mercadería	
11.2 Equipos	11.2.1 Emplazamiento y protección de los equipos(Ubicación y protección del equipamiento)	NO	Una correcta ubicación de los equipos disminuirá el riesgo de amenazas y peligros ambientales para los equipos.	Centro de Datos Principal / Enlace/contingenica Politica de escritorio y pantalla limpia
	11.2.2 servicios suministro(Elementos de soporte)	NO	CBC trabaja bajo la modalidad remota	
	11.2.3 Seguridad en el cableado	NO	Se debe proteger el cableado de energía y comunicaciones para evitar tanto daños como interferencias	Cableado estructurado, equipos ubicados en racks, canaletas,
	11.2.4 Mantenimiento de equipo	SI	Programar un mantenimiento periódico de los equipos a fin de mantener la disponibilidad de la información y evitar daños futuros que puedan ocasionar pérdida de información.	INS.05 Mantenimiento preventivo de Equipos de computo INS.010 Mantenimiento buzo de correos en el servidor
	11.2.5 remocion(Retiro) de activos	NO	Debe existir reglas de uso para los equipos fueras de las instalaciones, así también contar con una aprobación apropiada que sea documentada. CBC no cuenta con un lugar especifico, ya que se trabaja de manera remota	Control físico de ingreso y salida de equipos
	11.2.6 Seguridad de equipamiento y los activos fuera de las instalaciones	SI	Deben existir políticas de uso aceptable y compromiso del empleado cumpliendo requisitos de seguridad y obligaciones para uso de los equipos fuera de las instalaciones.	
	11.2.7 Disposicion o reutilización segura de equipos	SI	Para prevenir la revelación de la información en la reasignación o eliminación de equipos, será necesario realizar un respaldo o borrado seguro de la información	INS.008 Copias de seguridad
	11.2.8 Equipo de usuario desatendido	SI	Debe existir un tiempo adecuado para establecer en estado de suspensión cuando el usuario está en inactividad.	POL.014 Política de escritorio y pantalla limpios
	11.2.9 Política de escritorio y pantalla limpios	SI	Es importante que existan políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas	POL.014 Política de escritorio y pantalla limpios

Figura 16

Aplicabilidad

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
12.1 Procedimientos y responsabilidades	12.1.1 Procedimiento de operación documentados	SI	Se deben documentar los procedimientos operativos y ponerlos a disposición de los demás.	seguridad de la información / Repositorio de documentos
	12.1.2 Gestión de cambios	SI	Es de importancia la existencia de un plan de control para gestionar los cambios en sistemas operacionales	PRO.004 Gestión de Cambios
	12.1.3 Gestión de la capacidad	SI	Para alcanzar un nivel óptimo respecto a la productividad de los sistemas es importante que se realice un seguimiento continuo del uso de recursos pata tomar medidas correctivas si fuese necesario	listar que recursos tenemos(sharepoint; power apps, drive) sistemas de informacion
	12.1.4 Separación de los entornos(ambientes) de desarrollo, prueba y operaciones	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	
12.2 Protección contra código malicioso	12.2.1 Controles contra código malicioso	SI	Es vital para garantizar la integridad de la información que se establezcan mecanismos o herramientas de detección de ataques y código malicioso.	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus,Antispyware)
12.3 Respaldo	12.3.1 Respaldo de la información	SI	Con la realización de copias de seguridad de la información se garantiza que la información esté disponible a todo momento especialmente en caso de que ocurran incidentes que la comprometan.	INS.004 Backup de Correo INS.007 Backup de información de SharePoint
12.4 Registro y monitoreo	12.4.1 Registro(logs) de evento	SI	Es importante registrar los problemas que ocurren relacionados con la seguridad de la información a fin de analizarlos y brindar soluciones más eficaces	aplica para el sistema
	12.4.2 Protección de la información de registros	SI	Debe existir un área donde se resguarden archivos de importancia para la empresa con la finalidad de accesos no autorizados.	FOR.043 Registro de Backup de Información
	12.4.3 Registros del administrador y operador	SI	Debe existir un control de las actividades del administrador y operador del sistema para llevar un registro y poder ser revisado periódicamente.	TODO estas funciones nos debe ayudar en la parte tecnica GABRIEL
	12.4.4 Sincronización de relojes	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	
12.5 Control de software de operación	12.5.1 Instalación del software en sistemas operacionales	SI	Es necesario políticas de instalación de software para que asegurar que sea probado, aprobado, permitido y mantenido en la producción teniendo soporte en los diferentes ordenadores existentes en la empresa.	TODO estas funciones nos debe ayudar en la parte tecnica GABRIEL
12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas	SI	Al obtener oportunamente información de ataques o vulnerabilidades el departamento de TICS está en la capacidad de tomar las medidas correctivas apropiadas.	Informe de fixes y actualización de software base
	12.6.2 Restricciones sobre la instalación de software	SI	La instalación de software está limitada al personal autorizado que ejecuta la acción adecuada.	Lista de software base
12.7 Consideraciones de la auditoría de los sistemas de información	12.7.1 Controles de auditoría de sistemas de información	SI	Es necesario que exista una política que requiera auditorias de seguridad de la información para garantizar la confidencialidad de la información, para ello debe tener herramientas de auditoria controladas.	Levantamiento de requisitos de auditoria en la FOR.007 Base de datos
13.1 Gestión de la seguridad de red	13.1.1 Controles de red	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
	13.1.2 Seguridad de los servicios de red	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	Control de Accesos
	13.1.3 segregacion(Separación) en las redes	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	Seguridad perimetral / Segregación de redes VLANs
13.2 Transferencia de información	13.2.1 Políticas y procedimientos de transferencia de información	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	
	13.2.2 Acuerdos sobre transferencia de información	NO	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.	aolica la politica/ permisos ya utorizacionm
	13.2.3 Mensajería electrónica	SI	Toda información relacionada con los procesos internos pasa por servidores de mensajería que el departamento de TICS tiene configuradas, por lo que es indispensable asegurar la integridad de la misma.	comunicados
	13.2.4 Acuerdos de confidencialidad o no divulgación	SI	Es importante documentar acuerdos de confidencialidad de la información con lo cual se garantiza la no divulgación y por tanto el uso inadecuado de la misma.	FOR.035 Compromiso de Seguridad de la Información

Figura 16

Aplicabilidad

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
12.1 Procedimientos y responsabilidades	12.1.1 Procedimiento de operación documentados	SI	Se deben documentar los procedimientos operativos y ponerlos a disposición de los demás.	seguridad de la información / Repositorio de documentos
14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de requisitos de seguridad de la informacion	SI	Se deben regir en las políticas, procedimientos y registros relacionados con el análisis de requisitos de seguridad para la adquisición de sistemas y software	Politicas Procedimientos Analisis de contexto
	14.1.2 Aseguramiento de servicios de aplicación en redes publicas	NO	No aplica, la empresa no ejecuta el comercio electrónico debido a eso no genera transacciones electrónicas.	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware) PAGINA WEB /SI TIENE HTPPS
	14.1.3 Protección de las transacciones de servicios de aplicación	NO	No aplica, la empresa no ejecuta el comercio electrónico debido a eso no genera transacciones electrónicas.	Seguridad perimetral (IPS,Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
14.2 Seguridad en procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.2 Procedimientos de control de cambios del sistema	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operativa	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.4 Restricciones en los cambios a los paquetes de software	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.5 Principios de ingeniería de sistema seguro	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.6 Entorno de desarrollo seguro	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.7 Desarrollo contratado externamente/tercerizado	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.8 Prueba de seguridad del sistema	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
	14.2.9 Prueba de aprobación del sistema	NO	No aplica, debido a que la empresa no desarrolla ningún tipo de software	
14.3 Datos de prueba	14.3.1 Protección de datos de prueba	NO	Es de vital importancia mantener una discreción por parte del personal encargado de las pruebas y garantizar la confidencialidad de la información	
15.1 Seguridad de la información en las relaciones con proveedores	15.1.1 Política de seguridad de la información para las relaciones con el proveedor	SI	Se debe contar con políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con suministradores que se involucran servicios de TICS.	politica/Bases del servicio Contratos
	15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor	SI	Los acuerdos que se produzcan con los suministradores es necesario documentarlos para tener una validez y compromiso de ambas partes.	Cláusulas de seguridad de la información en contratos con los proveedores
	15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones	SI	Es importante que exista una validación de los requisitos de seguridad de los productos o servicios adquiridos y tener un control de rastreo del origen del producto o servicio.	GESTION DE COMPRAS

Figura 16

Aplicabilidad

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN	DOCUMENTACIÓN
15.2 Gestión de entrega del servicio del proveedor	15.2.1 Monitoreo(Supervisión) y revisión de los servicios del proveedor	SI	El departamento de TICS debe monitorizar los servicios prestados por terceros para evitar el riesgo de información.	GESTION DE PROVEEDORES -TI
	15.2.2 Gestión de cambios a los servicios del proveedor	SI	Los cambios en los servicios prestados por terceros con el hecho de estar ligados con la información deben	PRO.004 Gestión de Cambios
16.1 Gestión de incidentes de seguridad de la información y mejora	16.1.1 Responsabilidades y procedimientos	SI	Es necesario establecer responsabilidades para garantizar una respuesta eficaz e inmediata a un determinado problema de seguridad que se pronuncie.	Proc. Gestión de Incidentes de Seguridad
	16.1.2 Informe de eventos de seguridad de la información	SI	Al momento de una ocurrencia de cualquier eventualidad, la notificación del problema al departamento de TICS permitirá brindar una solución inmediata.	Registro(formato) Gestión de Incidentes de Seguridad
	16.1.3 Informe de debilidades de seguridad de la información	SI	Es vital que existan mecanismos de notificación de puntos débiles en la seguridad.	Proc. Gestión de Incidentes de Seguridad
	16.1.4 Evaluación y decisión sobre los eventos de seguridad de informacion	SI	Con la clasificación de incidentes de seguridad permitirá dar una solución eficaz a aquellos con mayor afectación para la empresa.	Proc. Gestión de Incidentes de Seguridad
	16.1.5 Respuesta ante incidentes de seguridad de la información	SI	Mediante el plan de contingencia se debe evaluar el manejo de incidentes que se puedan pronunciar.	Proc. Gestión de Incidentes de Seguridad
	16.1.6 Aprendizaje de los incidentes de seguridad de la info	SI	Con la documentación de los incidentes producidas se pueden identificar incidentes de impacto con el fin de evitar recurrencias.	Proc. Gestión de Incidentes de Seguridad
	16.1.7 Recolección de evidencia	SI	Con la recolección de evidencias de los incidentes hace de forma competente a la empresa o terceros capacitarse en área con procesos y herramientas adecuadas.	Proc. Gestión de Incidentes de Seguridad
17.1 Continuidad de la seguridad de informacion	17.1.1 Planificación de la continuidad de la seguridad de la información	SI	Para garantizar la continuidad de la seguridad de la información la empresa realice una planificación de las actividades empresariales, documentar los procesos y controles que permitan solucionar inconvenientes en un futuro cercano.	Plan de contingencia TI
	17.1.2 Implementación de la continuidad de la seguridad de la información	SI	En la continuidad de la seguridad de información debe ser implementado de forma que se puedan restaurar los	
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la informacion	SI	Debe existir un método de pruebas del plan de continuidad dando resultados reales.	Informe técnico de pruebas de contingencia
17.2 redundancias	17.2.1 instalaciones de procesamiento de la informacion	SI	Se den identificar los requisitos de disponibilidad de servicios para mantener un continuo procesamiento de Información con capacidades de recuperación	Centro de Datos Principal / Centro de Datos Alterno
18.1 Cumplimiento con requisitos legales y contractuales	18.1.1 Identificación de requisitos contractuales y legislacion aplicables	SI	Deben existir políticas acerca del cumplimiento garantizado de requisitos legales manteniendo un registro de cumplimiento de todas las obligaciones,expectativa legales, reglamentarias y contractuales.	Matriz de requisitos legal/ Identificación de Requisitos de Seguridad de la Información
	18.1.2 Derechos de propiedad intelectual	SI	Es necesario establecer políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento.	Política de Administración de Software
	18.1.3 Protección de los registros	SI	Deben promoverse buenas prácticas respecto a la protección por pérdida, destrucción, amenaza …, de registros importantes de la institución.	Control de Documentos
	18.1.4 Privacidad y protección de datos personales	SI	Debe existir un mecanismo para instruir al personal en el manejo de información debido a que por ética se debe garantizar la privacidad y la protección de la información de carácter personal	Controles de seguridad aplicables a las bases de datos de carácter personal
	18.1.5 Regulación de los controles criptográficos	SI	Debe existir una política que cubra actividades relacionadas con importación/exportación de material criptográfico, con requisitos legales y reglamentarios	
18.2 Revisiones de seguridad de la informacion	18.2.1 Revisión independiente de la seguridad de la información	SI	Es necesario revisar de manera individual políticas, objetivos de control y demás procesos de seguridad de	Auditorías Internas / Externas del SGSI
	18.2.2 Cumplimiento con las normas y políticas de seguridad de la informacion	SI	El departamento de TICS deberá asignar un responsable en el área de seguridad de información que deberá revisar periódicamente el cumplimiento de políticas, procesos, normas y demás mecanismos de seguridad implementados.	formato de Medición de Procesos y Controles del SGSI
	18.2.3 Revision(Verificación) del cumplimiento técnico	SI	Para una mejor administración en la gestión de seguridad es preciso la realización de una auditoría interna para garantizar que se cumplen adecuadamente los procesos de seguridad.	formato de Medición de Procesos y Controles del SGSI

VI.9. ANEXO 7. FOR.002 Objetivos e indicadores

Figura 17

Objetivos e indicadores de CBC

FORMATO																			Código : FOR.002	
OBJETIVOS E INDICADORES DEL SISTEMA INTEGRADO DE GESTIÓN																			Fecha: 04/02/21	Versión: 03
Revisión: 4																				
Actualizado: 8/09/2021																				
Política	**Objetivo**	**Indicadores**	**Meta**	**Formato / Fuente de datos**	**Frecuencia de medición**	**Responsable**	**ENE**	**FEB**	**MAR**	**ABR**	**MAY**	**JUN**	**JUL**	**AG**	**SEP**	**OCT**	**NOV**	**DIC**		
Satisfacer a nuestros clientes, cumpliendo con los requisitos contractuales y legales	O1. Mejorar la percepción del cliente acerca del servicio brindado.	Encuesta de Servicio de capacitaciones	≥85%	Encuestas. Base de datos de Encuestas de Satisfacción	Cierre del proyecto	Procesos SIG	83%	86%	88%	85%	98%									
		Servicio de capacitación Eco e-learning	≥85%	Encuestas. Base de datos de Encuestas de Satisfacción	Cierre de capacitación	Procesos SIG														
		Encuesta de Satisfacción en Auditoría/Inspección, Asesoría	≥85%	Encuestas. Base de datos de Encuestas de Satisfacción	Cierre del proyecto	Procesos SIG	85%	83%	85%	80%	84%									
	O2. Cumplir con los tiempos en los Entregables	# entregables en el tiempo establecido / total de entregables x 100	≥ 90%	Base de datos de Control de Actividades	Mensual	Procesos SIG	75%	75%	80%	100%					90%					
	O3.Formalizar temas contractuales con el clientes	# ACS o Contratos u otro con clientes / # Total con clientes x 100	≥ 80%	Contratos OS	Mensual	Socio Principal	76%	82%	82%	82%					100%					
Cumplir con los requisitos legales y otros aplicables, que impacten al Sistema Integrado de Gestión.	O4. Cumplir con los requisitos legales y otros	Requisitos legales implementados en el período establecido / Total de Requisitos legales x 100%	90%	Matriz de Requisitos Legales	Trimestral	Business Partner	NA	NA	90%											
Promover la protección de la seguridad y salud de todos nuestros colaboradores mediante la prevención de las lesiones, dolencias, enfermedades e incidentes relacionados con el trabajo.	O5. Mejorar los indicadores de accidentabilidad de la organización	Índice de Accidentabilidad (IA) = IF*IS / 1000	0	Registro de accidentes	Mensual	Procesos SIG/ Business Partner														
	O6. Controlar la gestión de las enfermedades profesionales de nuestros trabajadores	Incidencia EP: (N° total de casos nuevos enfermedades profesionales / N° total de población expuestos) X 1000000	0	Registro de accidentes	Mensual	Procesos SIG/ Business Partner														
		Prevalencia EP: (N° total de casos de enfermedades profesionales / N° toral de población expuesta) x 1000000	0	Registro de accidentes	Mensual	Procesos SIG/ Business Partner														
	O7. Controlar los riesgos laborales de los puestos de trabajo de la organización	IPERC. Control operacional: (N° acciones ejecutadas del Control Operacional del IPERC/ Total de acciones) x 100%	70%	IPERC	Mensual	Procesos SIG/ Business Partner														
Preservar la confidencialidad, integridad y disponibilidad de la información de nuestras partes interesadas.	08. Controlar los riegos de información en los proceso de la empresa	RIESGOS SI. Control operacional: (N° acciones ejecutadas del Control Operacional del RIEGOS SI/ Total de acciones) x 100%	70%	Matriz de RIESGOS SI	Mensual	Procesos SIG/ Business Partner														
	0.9.Controlar las amenzas en la seguridad de la información	Porcentaje de ataques informáticos que impidieron la prestación de algun servicio	0	Registros de incidencias	Mensual	Procesos SIG/ Business Partner														
Gestionar los riesgos de la organización, implementando controles que aseguren la continuidad del negocio	0.10. Implementar los controles de la Gestión de Riesgos y oportunidades (Enfoque Preventivo)	# acciones ejecutadas dentro del Plazo / # acciones programadas x 100	≥ 75%	Matriz de Riesgos y Oportunidades	Mensual	Procesos SIG/ Business Partner	25%	30%	40%	45%										
Asegurar los mecanismos de formación, comunicación, escucha activa, participación y consulta a todos los colaboradores y/o partes interesadas.	O11. Incrementar las competencias profesionales del personal	Cursos realizados / Cursos programados x 100	100%	Programa de Capacitación anual	Mensual	Psicología	100%	100%	100%	N.A	N.A	N.A	N.A	100%	N.A	N.A	0%	0%		
	O12. Mantener la gestión del conocimiento.	# Porcentaje de cumplimiento del programa de investigaciones	100%	Programa de Capacitaciones		Administración	N.A	N.A	N.A	100%	100%	N.A	33%	67%	50%	67%	0%	0%		
		# Porcentaje de cumplimiento del programa de comunicaciones	100%	Programa de investigaciones	Mensual	Administración	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	0%		
	O13. Gestionar adecuadamente los proveedores	Evaluación Promedio de la calificación de los Proveedores Críticos para la Gestión x 100	≥ 75%	Base de dato de partes interesadas (Hoja Proveedores)	Semestral	Procesos SIG/ Business Partner				82%										
	O14. Formalizar temas contractuales con el Proveedor	# ACS o Contratos con proveedores / # Total con proveedores x 100	100%	Proveedores AC	Trimestral	Procesos SIG/ Business Partner	NA	NA	43%						100%					
Mejorar continuamente nuestro sistema integrado de gestión, en el cumplimiento de: los procesos, la eficiente gestión de recursos financieros y los objetivos estratégicos de la organización.	015. Asegurar el cumplimiento de plan de acción de una no conformidad (NC)	# acciones correctivas y oportunidades de mejora cerradas en plazo / total acciones correctivas y oportunidades de mejora x 100	≥ 90%	Base de datos de Acciones Correctivas	Mensual	Procesos SIG	100%	100%	100%	100%	100%									
	0.16. Asegurar el cumpliento del programa anual del SIG	# actividades realizadas / # actividades programadas	≥ 90%	Programa anual SIG	Anual	Procesos SIG	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	29.4%		

VI.10. ANEXO 8. POL.008 Caracterización de procesos

Figura 18

Caracterización de procesos

	POLITICA	Código: POL.008	
Core Business Corp.	CARACTERIZACIÓN DE PROCESOS	Fecha: 7/10/2021	Versión: 3
		Página 12 de 13	

PROCESO	Infraestructura	**REQ ISO 9001**	7.1 / 7.5 / 8.5.3 / 9.1
OBJETIVO	Mantener la infraestructura para la operación de los procesos de Core Business Corp.	**REQ ISO 45001**	7.1 / 7.5 / 9.1
		REQ ISO 27001	7.1 / 7.5 / 9.1
RESPONSABLE DEL PROCESO	Business Partner		

PROCESO DE ENTRADA	INSUMO / ENTRADA	CRITERIOS Y METODOS	MEDIDAS DE CONTROL	PRODUCTO / SALIDA	PROCESO DE SALIDA
• Planificación estratégica • Gestión Comercial • Gestión Financiera • Asesoría • Recursos Humanos • Proveedores • Todos los procesos	• Solicitud o requerimiento de las áreas usuarias	• PRO.015 Infraestructura tecnológica • INS.005 Mantenimiento preventivo de equipos	• Comités internos.	• Mantenimiento preventivo de Equipos de cómputo • Back up • Creación o eliminación de cuentas de correo	• Planificación estratégica • Gestión Comercial • Gestión Financiera • Asesoría • Recursos Humanos • Proveedores • Todos los procesos

RECURSO HUMANO	FINANCIERO	TECNOLÓGICO	AMBIENTE DE TRABAJO / EPP
• Business Partner • Consultor	Facturación de la organización (Documentos internos)	Laptops, internet, equipos de comunicación (telefonía)	No se cuenta con ambiente físico, trabajo remoto.

INDICADOR	FÓRMULA	RESPONSABLE	FRECUENCIA DE MEDICIÓN
Cumplimiento del Programa de soporte informático	% cumplimiento del programa	Business Partner	Mensual

Figura 18

Caracterización de procesos

	POLITICA	Código: POL.008	
Core Business Corp.	CARACTERIZACIÓN DE PROCESOS	Fecha: 7/10/2021	Versión: 3
		Página 5 de 13	

PROCESO	Asesorías	**REQ ISO 9001**	8.1 / 8.2 / 8.4 / 8.5 / 8.6 / 8.7
OBJETIVO	Realizar el planeamiento, ejecución y evaluación de los servicios de asesoría.	**REQ ISO 45001**	8.1 / 8.2
		REQ ISO 27001	8.1 / 8.2
RESPONSABLE DEL PROCESO	Consultor Líder		

PROCESO DE ENTRADA	INSUMO / ENTRADA	CRITERIOS Y METODOS	MEDIDAS DE CONTROL	PRODUCTO / SALIDA	PROCESO DE SALIDA
• Gestión de Recursos Humanos • Gestión de Proveedores • Gestión de Recursos Financieros • Gestión Comercial • Sistema de Gestión	• Requerimiento de servicio de cliente • Especificaciones del contrato y/o orden de servicio	• PRO.016 Auditoria, Inspección y Asesoría	• Comités con el cliente. • FOR.031. Encuesta Satisfacción de Asesoría • FOR.040 Planeación del Servicio • FOR.045 Evaluación de Proyectos	• Aceptación del servicio • Entregables del servicio según plan de proyecto	• Proceso de Sistema Integrado de Gestión

RECURSO HUMANO	FINANCIERO	TECNOLÓGICO	AMBIENTE DE TRABAJO / EPP
• Líder Consultor • Consultores • Business Partner	Facturación de la organización (Documentos internos)	Laptops, internet, equipos de comunicación (telefonía)	Equipos de protección personal (De ser el caso)

INDICADOR	FÓRMULA	RESPONSABLE	FRECUENCIA DE MEDICIÓN
Cumplimiento de tiempos de entregables	# entregables en el tiempo establecido / total de entregables x 100	Consultor Líder	Mensual
Satisfacción del servicio	Encuesta de satisfacción	Responsable de Desarrollo de Procesos	Acorde PRO.006. Procedimiento medición de la satisfacción del cliente.

VI.11. ANEXO 9. FOR.003 Programa anual del SIG

Figura 19

Programa anual 2021

	Programa anual SIG 2021						CODIGO: FOR.003	
							FECHA: 03/09/2021	VERSIÓN: 02

Revision: 4
Fecha de actualización: 30/09/21

OBJETIVOS:	1. Recurso Tegnológico: computadora, inventarios de equipos 2.Recurso Humano: Personal Interno y externo, procedimientos internos. 3. Recurso economico: Presupuesto

PROYECTOS	AVANCE	INICIO DEL	FIN DEL PROYECTO
Proyecto 1: Auditoria de seguimiento ISO 9001:2015 Proyecto 2: Certificación ISO 27001 Proyecto 3: Certificación ISO 45001	28%	6/03/2021	20/12/2021

Nombre de tarea	% Avanc	ESTADO REALIZAD	ESTADO PROCESO	ESTADO PENDIENT	ESTADO	EVIDENCIAS	Responsable interi	Responsable de la ejecució
Planificación	64.0%	60.0%	4.0%	36.0%				
1ª Reunión de apertura (Presentación del programa SIG)	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	PA/LA	DV
Levantamiento de Observaciones para realizar la actualización de la Web C	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	PA/LA	DV
1ª Reunión de comité de SIG	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	PA/LA	PA
2ª Reunión de comité de SIG	0.0%	0.0%	0.0%	0.0%	PENDIENTE	Acta de Comité	PA/LA	PA
3ª Reunión de comité de SIG	0.0%	0.0%	0.0%	0.0%	PENDIENTE	Acta de Comité	PA/LA	PA
4ª Reunión de comité de SIG	0.0%	0.0%	0.0%	0.0%	PENDIENTE	Acta de Comité	PA/LA	PA
Capacitación en ISO 27001	100.0%	100.0%	0.0%	0%	REALIZADO	Registro de capacitación	PA	PA
Coordinación	100.0%	100.0%	0.0%	0%	REALIZADO	Correo	PA	PA
Ejecución de la capacitación	100.0%	100.0%	0.0%	0%	REALIZADO	Registro de capacitación	PA	PA
Asesorías externas en ISO 27001(quincenales/Fechas acordadas)	40.0%	0.0%	40.0%	0%	EN PROCESO	Correo	DV	JL
Implementación	53.6%	32.5%	21.0%	46.4%				
Procesos Estratégicos	50.1%	32.3%	17.8%	49.9%				
Sistema Integrado de Gestión	43.0%	27.1%	16.9%	56.0%				
Revisión y actualización de POL.001 Política de Excelencia Organizacional	100.0%	100.0%	0.0%	0%	REALIZADO	Política	LA	LA
Aprobación de POL.001 Política de Excelencia Organizacional	100.0%	100.0%	0.0%	0%	REALIZADO	Correo	DV	DV
Publicación de POL.001 Política de Excelencia Organizacional	100.0%	100.0%	0.0%	0%	REALIZADO	Correo	LA	SN/VP
Reunión para la definición de Objetivos e Indicadores de SIG	100.0%	100.0%	0.0%	0%	REALIZADO	correo	PA/LA	DV
Revisión, actualización y medición del FOR.002 Objetivos e indicadores	100.0%	100.0%	0.0%	0%	REALIZADO	Formato	LA	LA
Aprobación del FOR.002 Objetivos e indicadores del SIG	100.0%	100.0%	0.0%	0%	REALIZADO	correo	DV	DV
1ª Seguimiento de los objetivos SIG por áreas	100.0%	100.0%	0.0%	0%	REALIZADO	Data de Objetivos por àr	LA	SN/MA/IH/DV/HD/PA
2ª Seguimiento de los objetivos SIG por áreas	80.0%	0.0%	80.0%	0%	EN PROCESO	Data de Objetivos por àr	LA	SN/MA/IH/DV/HD/PA

Figura 19

Programa anual 2021

	Programa anual SIG 2021						CÓDIGO: FOR.003	
							FECHA: 03/09/2021	VERSIÓN: 02

Revision: 4
Fecha de actualización: 30/09/21

OBJETIVOS:	1. Recurso Tegnológico: computadora, inventarios de equipos 2.Recurso Humano: Personal Interno y externo, procedimientos internos. 3. Recurso economico: Presupuesto

PROYECTOS	**AVANCE**	**INICIO DEL**	**FIN DEL PROYECTO**
Proyecto 1: Auditoria de seguimiento ISO 9001:2015 Proyecto 2: Certificación ISO 27001 Proyecto 3: Certificación ISO 45001	30%	6/09/2021	20/12/2021

Nombre de tarea	**% Avanc**	**ESTADO REALIZAD**	**ESTADO PROCESO**	**ESTADO PENDIENT**	**ESTADO**	**EVIDENCIAS**	**Responsable interi**	**Responsable de la ejecuci**
Planificación	**64.0%**	**60.0%**	**4.0%**	**36.0%**				
Infraestructura-SI	**55.2%**	**42.9%**	**16.1%**	**44.8%**				
Reunión de coordinación para definición de Politicas	100.0%	100.0%	0.0%	0%	REALIZADO	Correo	PA/LA/HD	PA/LA/HD
Comunicado de Oficial de SI	100.0%	100.0%	0.0%	0%	REALIZADO			
Elaborar una formato de aplicabilidad de SI	100.0%	100.0%	0.0%	0%	REALIZADO			
Aprobar una formato de aplicabilidad de SI	100.0%	100.0%	0.0%	0%	REALIZADO			
Politica de seguridad de dispositivos moviles y Teletrabajo	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	
Politica de Control de Acceso	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	
Politica sobre el uso de controles Criptograficos	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	
Politica de Escritorio Limpio y pantala limpia	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	
Politica de seguridad de la inf. Para las relaciones con los proveedores	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	
Politica y procedimiento de transferencia de la informacion	100.0%	100.0%	0.0%	0%	REALIZADO	Politica	PA/LA/HD	PA/LA/HD
Aprobación	100.0%	100.0%	0.0%	0%	REALIZADO	Acta de Comité	DV	DV
Elaborar el inventario de Activos	100.0%	100.0%	0.0%	0%	REALIZADO	Formato	LA/PA	LA
Aprobacion del FOR 062 inventario de Activos	100.0%	100.0%	0.0%	0%	REALIZADO	Correo	LA/PA	LA
Asesoría	**31.4%**	**16.1%**	**35.0%**	**48.3%**				
Reunión para la Revisión de procedimientos, formatos , etc.	100.0%	100.0%	0.0%		REALIZADO	Correo	PA/LA	IH/MA

VI.12. ANEXO 10. Acta de Comité

Figura 20

Acta de Comité

	FORMATO	Código: FOR.004	
	ACTA DE COMITÉ	Fecha de publicación: 26/01/2021	Versión: 1

FECHA : 11/11/21

MODALIDAD : Remoto

OBJETIVO : Seguimiento SI

HORA : 3:15pm

ASISTENTES :

- Dante Velásquez Aliaga-Socio Principal
- Lucero Arana Walde- Responsable de desarrollo de procesos SIG

AGENDA:

- Acuerdos para el proceso de implementación SI

PLANES DE ACCIÓN

ACCIONES DE IMPLEMENTACIÓN	RESP	FECHA EJECUCIÓN	ESTADO
1. Compromiso de confidencialidad de CBC para los clientes	LA	11/11/21	Cerrado
2. Actualizar el Compromiso del colaborador	LA	11/11/21	Cerrado
3. Elaborar el reglamento interno de trabajo	LA	11/11/21	Cerrado
4. Política de proveedores SIG (calidad de servicio, corrupción y seguridad de la información)	LA	11/11/21	Cerrado
5. Elaborar una política de control de accesos	LA	11/11/21	Cerrado
6. Lista de sanciones	LA	11/11/21	Cerrado
7. Comunicados(Tips para concientizar a los colaboradores)	LA	11/11/21	Cerrado
8. Se definido el tipo de trabajo - Trabajo remoto	DV	11/11/21	Cerrado
9. Elaborar el plan de contingencia	LA	11/11/21	Cerrado

	FORMATO	Código: FOR.004	
	ACTA DE COMITÉ	Fecha de publicación: 26/01/2021	Versión: 1

- Reglamento interno, con apoyo de Solange Nieto, con el listado sanciones teniendo en cuenta su criticidad.
- Política de proveedores teniendo en cuenta la calidad de servicio, corrupción (el cual debe brindarnos Paul Aliaga) y seguridad de la información, contando con una política integrada.
- Elaborar el plan de contingencia, para ello solicitar a Dante Velásquez un requerimiento de proveedor para que se encarga de la revisión de dicho documento. Teniendo en cuenta: Robo /hurto/ hackeo/ perdida de equipos(criticidad)

Comunicados

Elaborar Tips sobre:

- ¿Conoces sobre los activos de información?
- ¿Qué es una amenaza?
- ¿Qué es un incidente SI?
- Controles a tener en cuenta para un trabajo remoto

Los cuales deben estar dentro del programa de comunicaciones.

Condición de trabajo

Se definido que se laborara en la condición de Trabajo remoto.

Indicador

Enviar el indicador correspondiente a:

Objetivo	Indicadores	Meta
O.3 Formalizar temas contractuales con el clientes	# ACS o Contratos u otro con clientes / # Total con clientes x 100	≥ 80%

Revisión de formatos para su aprobación

- POL.008. Caracterización de procesos
- FOR.015 análisis de contexto
- POL.003 Alcance
- IN5.001 Elaboración estratégica
- FOR.062 Inventario de Activos de información
- FOR.063 Matriz de riesgos de SI
- FOR.064 Aplicabilidad

IV. **PRÓXIMA REUNIÓN**

VI.13. ANEXO 11. Políticas de seguridad de la información

Figura 21

Políticas de Seguridad de la Información

	POLÍTICA	Código: POL.011	
	POLÍTICA DE DISPOSITIVOS MÓVILES	Fecha de publicación: 22/09/2021	Versión: 01

1. **OBJETIVO**

El presente documento define la política para el uso adecuado de dispositivos móviles por parte de los colaboradores de Core Business Corp. S.A.C

2. **ALCANCE**

Aplica a todo los colaboradores y proveedores de CORE BUSINESS CORPORATION S.A.C

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES**

- **Antivirus:** Software de detección y eliminación de virus informáticos conocidos como "malware".
- **Dispositivos Móviles:** dentro de los dispositivos móviles se encuentran: Celulares o Móviles, Laptops o Tablet, USB, Discos Duros Externos.
- **Discos duros externos:** Unidad removible con mayor capacidad de almacenamiento de datos lógico, en comparación con las memorias USB.

5. **RESPONSABILIDADES**

La responsabilidad por la implantación, ejecución y control de esta política está a cargo del Oficial de la Seguridad de la Información.

6. **POLÍTICA**

La jefa de administración y finanzas solicitará a cada colaborador leer y firmar el FOR.036 Compromiso de la seguridad de Información. De acuerdo a ello se le dará a conocer la presente política:

La Alta Dirección con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información sobre el dispositivo móvil, dispone a cumplir y a seguir los siguientes lineamientos:

- Utiliza tus dispositivos móviles solo para fines de trabajo. enfatizar sobre la laptop
- Ten actualizado el antivirus en tu laptop, móvil, Tablet entre otros dispositivos móviles.
- Cuando uses algún dispositivo de almacenamiento externo deberás ejecutar un análisis de antivirus para confirmar que el dispositivo no cuente con malware o algún virus informático.
- Está prohibido el almacenamiento, instalación de software y aplicaciones que no se apunten a las tareas asignadas.
- Bloquea tus dispositivos con alguno de estos mecanismos de autentificación: PIN, clave, patrón, etc.
- Se cuidadoso a la hora de estar en lugares públicos, evita que terceros revisen tus dispositivos de trabajo.
- Informa de manera inmediata a tu jefe acerca del mal uso, perdida, daño o robo de cualquier dispositivo de la empresa.
- Se deben evitar la utilización de dispositivos móviles en lugares donde se perciba condiciones insegura, para evitar pérdidas y robos.

Figura 21

Políticas de Seguridad de la Información

	POLÍTICA	Código: POL.012	
	POLÍTICA DE TRABAJO REMOTO	Fecha de publicación: 22/09/2021	Versión: 01

1. **OBJETIVO**

El presente documento establece una política de trabajo remoto para que los colaboradores de Core Busines Corp. S.A.C puedan prestar sus servicios, evitando la propagación de la COVID-19 y como medida preservar la salud de los colaboradores

La presente política establecer directrices que le permitan tanto CBC como a los colaboradores tener claras las condiciones de esta nueva modalidad de trabajo

2. **ALCANCE**

Aplica a todo los colaboradores y proveedores de CORE BUSINESS CORPORATION.S.A.C

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información
- Guía de aplicación para trabajo remoto

4. **DEFINICIONES**

- **Trabajo remoto:** responde puntualmente a una medida ocasional, temporal y excepcional donde las empresas autorizan a algunos de sus empleados a trabajar desde casa durante esta situación de emergencia sanitaria.
- **Antivirus:** Software de detección y eliminación de virus informáticos conocidos como "malware".
- **Discos duros externos:** Unidad removible con mayor capacidad de almacenamiento de datos lógico, en comparación con las memorias USB.
- **USB:** Unidad de almacenamiento externo de información

5. **RESPONSABLES**

La Alta dirección asegura la implementación y el cumplimiento de la Política de Trabajo Remoto.

6. **POLÍTICA**

La Alta Dirección protege la información de amenazas como el acceso no autorizado, alteración indebida o software malicioso con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información, por ello se debe seguir los siguientes lineamientos:

- Establecer ambientes físicos seguros para realizar tus funciones ; elige un lugar libre de documentos y otras condiciones que puedan afectar el trabajo seguro.
- Conéctate desde accesos a internet confiables, no públicos o gratuitos.
- Debes asegurarte que todo dispositivo de almacenamiento externo (USB, Discos Duros portables, entre otros) a un equipo de cómputo, laptop y Tablet de que sea analizado por el software antivirus.
- Debes bloquear tu equipo cuando das una pausa a tus funciones desde el cual te conectas.
- Se prudente al abrir archivos adjuntos de correo eléctrico, ya que estos podrían contener virus por ello debes eliminarlo y reportarlo inmediatamente.
- Limita el uso personal del correo electrónico, internet y teléfono a momentos en los que no interfieran en tu trabajo.
- Evita que tus familiares, amistades entre otras personas usen tus dispositivos de medio de trabajo.

Figura 21

Políticas de Seguridad de la Información

	POLÍTICA	Código: POL.013	
	POLÍTICA DE CONTROL DE ACCESO	Fecha de publicación: 22/09/2021	Versión: 01

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para controlar el acceso a la información mantener y asegurar un nivel de protección adecuado para los activos de información de Core Business Corporation S.A.C

2. **ALCANCE**

Aplica a todo los colaboradores de CORE BUSINESS CORPORATION S.A.C

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **POLÍTICAS RELACIONADAS**

- POL.011 Política Dispositivos móviles
- POL.012 Política Trabajo remoto
- POL.013 Política Control de acceso
- POL.014 Política Escritorio limpio y pantalla limpia
- POL.015 Política de proveedores

5. **POLÍTICA**

La Alta Dirección considera que el acceso a la información y a los recursos debe ser controlado con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información, de acuerdo a ello se debe cumplir con los siguientes lineamientos:

- Accede sólo a la información que necesitas para el desarrollo legítimo de tus funciones y actividades.
- Eres responsables del uso adecuado de accesos y restricciones, evita brindar acceso a personas que no tengan nada que ver con tus funciones como familiares, amigos, entre otros externos a CBC.
- Los dispositivos móviles como laptop, tablet, celulares entre otros deben tener mecanismos de seguridad por medio de técnicas de autenticación y autorización, bloquea tus dispositivos y equipos con PIN, patrones, entre otros.
- Informa sobre los eventos y actividades críticas llevadas a cabo por los usuarios al Oficial de seguridad de la información.
- Evita ingresar a las plataformas de Outlook, E-Core learning entre otras con contraseñas predecible o fácil de adivinar, mejóralas con las siguientes indicaciones: longitud mínima de 8 caracteres cumpliendo una combinación de números, símbolos, letras mayúsculas, minúsculas. Ejemplo: Xm1LPn%m.
- Tu contraseña no debe ser escrita o almacenada en lugares visibles o cerca de los sistemas a los cuales permiten el acceso.
- Recuerda que al término de tu contrato se revocará según el caso el acceso a los diferentes sistemas.
- Está prohibido el uso de cuentas genéricas para acceder a los sistemas y aplicaciones, recuerda que todo es con el correo y accesos corporativo asignados.
- Todos tus equipos de trabajo deben ser apagados una vez que culmines con tu jornada de trabajo.

Figura 21

Políticas de Seguridad de la Información

	POLÍTICA	Código: POL.014	
	POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	Fecha de publicación: 23/09//2021	Versión: 01

1. **OBJETIVO**

El presente documento define la política para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en el lugar de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión digitalización de documentos, durante y fuera del horario laboral que utilizan los colaboradores de CBC.CORE BUSINESS CORP. SA.C

2. **ALCANCE**

Aplica a todo los colaboradores y proveedores de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES:**

- **Medio Extraíble:** Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos.
- **Lugar de Trabajo:** Lugar dispuesto por los colaboradores o proveedores para la realización de las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.

5. **RESPONSABILIDADES:**

El oficial de seguridad y la Alta Dirección es el responsable de asegurar la por la implantación, ejecución y control de esta política

6. **POLÍTICA**

6.1. POLÍTICA DE ESCRITORIO LIMPIO

La alta dirección expresa su compromiso en el desarrollo de una cultura de seguridad y prevención a la hora de realizar las actividades de CBC, con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información.

- Organiza tu escritorio, evita tener documentos en desorden, cables tirados, objetos no dispensables para realizar tus funciones, tu lugar de trabajo debe permanecer despejado y libre de documentos físicos y/o medios extraíbles que contengan información de CBC.
- Debes ubicar y proteger tu laptop, celulares, impresoras para reducir los riesgos de amenazas, así como las oportunidades para el acceso no autorizado.
- Protege los documentos y dispositivos removibles de almacenamiento de información, guárdalos en lugares no visibles.
- Cuando imprimas debes retirar inmediatamente de la impresora todo documento que contenga información perteneciente y sensible de CBC.

6.2. POLÍTICA DE PANTALLA LIMPIA

La Alta dirección expresa su compromiso en el desarrollo de una cultura de seguridad de la información y prevención a la hora de realizar las actividades de CBC, con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información.

- Siempre que te ausentes de tu lugar de trabajo, deberás bloquear o suspender tu laptop, por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L.
- La pantalla de la laptop (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.
- Al finalizar la jornada de trabajo, debes guardar en la nube en el repositorio asignado Share o drive la información confidencial o de uso interno de CBC.
- Debes, deberás guardar en un lugar seguro cualquier documento físico, USB, Laptop que contenga información de CBC, Siempre que te ausentes de tu área de trabajo
- Guarda en SharePoint la documentación digital, ingresa a equipos y visualizaras la carpeta correspondiente de acuerdo a tu responsabilidad.
- Avisar de cualquier incidente al Oficial de seguridad

Figura 21

Políticas de Seguridad de la Información

	POLÍTICA	Código: POL.015	
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	Fecha de publicación: 23/09/2021	Versión: 01

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para garantizar la protección de los activos de información que son accesibles a los proveedores.

2. **ALCANCE**

Aplica a los proveedores de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES:**

- **Antivirus:** Software de detección y eliminación de virus informáticos conocidos como "malware".
- **Dispositivos Móviles:** dentro de los dispositivos móviles se encuentran: Celulares o Móviles, Laptops o Tablet, USB, Discos Duros Externos.
- **Lugar de Trabajo:** Lugar dispuesto por los colaboradores o proveedores para la realización de las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.
- **Software:** está compuesto por un conjunto de aplicaciones y programas diseñados para cumplir diversas funciones dentro de un sistema. Ejemplo: Microsoft Windows, Microsoft Word, Google Chrome, Adobe Photoshop, Microsoft Excel entre otros.

5. **RESPONSABILIDADES:**

La responsabilidad por la implantación, ejecución y control de esta política está a cargo del Oficial de la Seguridad de la Información.

6. **POLÍTICA**

6.1. Seguridad de la Información en las Relaciones con los Proveedores

La alta dirección con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad de la información, de acuerdo a ello se debe cumplir con los siguientes lineamientos:

- El oficial de seguridad de la información registrara tus datos en el formato de proveedores con los datos necesarios para el servicio.
- Cuenta con un lugar de trabajo adecuado para la realización de tus funciones.
- Si haces uso de un dispositivo móviles asegúrate que cuenten con el antivirus actualizado asi como los sofware que utilizaras para los proyectos asignados.
- El acceso a los documentos físicos como digitales de los clientes debe ser autorizado por el oficial de seguridad de la información.
- Al culminar tus labores como auditor o inspector evita divulgar los asuntos vistos en la empresa a externos.
- Si manejas información, recursos o servicios tecnológicos, debe protegerlos del acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo.
- Todo contacto o conocimiento de información de CBC debe guardar absoluta confidencialidad, esta obligación permanece vigente 2 años posterior a la extinción del contrato.

VI.14. ANEXO 12. MOF

Figura 22

Manual de organización y funciones

Core Business Corp.	MANUAL	Código: MAN.001	
	MANUAL DE ORGANIZACIÓN Y FUNCIONES	Fecha: 16/04/2021	Versión: 1

Versión	1	Fecha de actualización	16/04/2021
Posición	**Socio Principal**		
Área	Gerencia General		
Jefe Inmediato	No aplica	Personal a cargo	• Jefe de Administración y Finanzas • Coordinador de Desarrollo de Procesos • Business Partner • Consultor Líder
Objetivo de puesto	Planear, dirigir y controlar las actividades de la empresa junto con los demás Jefes funcionales. Liderar la Gestión Comercial, ser responsable por los resultados de las operaciones y el desempeño organizacional. Pertenece a la Alta Dirección		
Funciones principales	•Liderar el proceso de planeación estratégica de la organización, determinando los factores críticos de éxito, estableciendo los objetivos y metas específicas de la empresa. •Gestionar los riesgos de la organización • Seleccionar personal competente y desarrollar programas de entrenamiento para potenciar sus capacidades •Revisar periódicamente el análisis financiero de la empresa. •Planear, dirigir, coordinar, controlar y evaluar estudios de mercados para la identificación y reconocimiento de nuevos clientes factibles del servicio. •Gestionar temas legales de acorde a la necesidad de la empresa. •Asegurar de que se establecen, implementan y mantienen los procesos necesarios para el sistema de gestión de la calidad. • Supervisar los procesos de Gestión Comercial en conjunto con la Administración. •Cumplir con las medidas de prevención relacionados a seguridad y salud en el trabajo y Seguridad de Información establecidas por el cliente. •Cumplir con los lineamientos del Sistema Integrado de Gestión (Calidad, Seguridad de la Información , y Seguridad y Salud en el Trabajo) de la organización. •Concientiza a todos los colaboradores sobre la Política de Excelencia Organizacional y Políticas SI. •Gestión Comercial • Elaborar las ofertas de valor para cada uno de los clientes. •Cumplir con las medidas de prevención relacionados a seguridad y salud en el trabajo establecidas por el cliente. •Apoyar a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.		

Ofimática	Word Avanzado	Excel Avanzado	Power Point Avanzado
Experiencia (Año, Sector, posiciones similares)	Experiencia mínima de 8 años		
Educación	Titulado en Administración, Gestión y Alta Dirección, Ingeniería Sistemas, Ambiental, Industrial o afines. (Obligatorio) • Maestría en Gestión de Riesgos: Seguridad y Salud Ocupacional. (Deseable) • MBA. (Deseable) • Maestría en Auditoría. (Deseable)		
Conocimientos Específicos (Formación)	• Auditor Líder ISO 9001, 45001, 37001, 27001		
Habilidades	• Liderazgo • Enfoque en resultados • Negociación • Servicio al cliente • Asertividad • Pensamiento crítico • Flexibilidad		

Figura 22

Manual de organización y funciones

Core Business Corp.	MANUAL	Código: MAN.001	
	MANUAL DE ORGANIZACIÓN Y FUNCIONES	Fecha: 16/04/2021	Versión: 1

Versión	1	Fecha de actualización	16/04/2021
Posición	**Consultor Líder**		
Área	Proyectos		
Jefe Inmediato	• Socio Principal • Business Partner	Personal a cargo	No aplica
Objetivo de puesto	Liderar el cumplimiento de todos los proyectos de clientes. Cumplir con los objetivos de los procesos de la operación de Core Business Corp.		
Funciones y responsabilidades principales	• Liderar la elaboración de los planes de los proyectos asignados. • Ejecutar los planes de proyectos de CBC. • Reuniones periódicas con el cliente con el fin de revisar es estatus de los proyectos. • Realizar inspecciones, capacitaciones, asesorías al cliente. • Gestionar con el Business Partner necesidades de asesorías especializadas. • Cumplir con las medidas de prevención relacionados a Seguridad y Salud en el Trabajo y Seguridad de la Información establecidas por el cliente. •Cumplir con los lineamientos del Sistema Integrado de Gestión (Calidad, Seguridad de la información, y Seguridad y Salud en el Trabajo) de la organización. • Concientizarse con la Política de Excelencia Organizacional y Politicas SI • Cumplir con la Política de Excelencia Organizacional y Politicas SI		

Ofimática	Word Intermedio	Excel Intermedio	Power Point Intermedio
Experiencia	• Mínimo cuatro años de experiencia en puestos y/o funciones similares. (Obligatorio)		
Educación	• Bachiller en Administración, Gestión y Alta Dirección, Ingeniería: Sistemas, Ambiental, Industrial, Química o afines (Obligatorio) • MBA, Maestría en Seguridad y Salud en el Trabajo, Maestría en Sistemas de gestión o afines (Deseable)		
Conocimientos Específicos (Formación)	• Contar por lo menos con un curso de Auditor Líder ISO 9001, 14001, 45001, 37001 (Obligatorio). • Deseable contar con 3 cursos de auditor líder • Deseable Especialización en Calidad, Seguridad, Medio Ambiente, Sistemas Integrados de Gestión. • Deseable Especialización en Gestión de Proyectos.		
Habilidades	• Liderazgo • Negociación • Servicio al cliente • Comunicación • Flexibilidad		

Figura 22

Manual de organización y funciones

Core Business Corp.	MANUAL	Código: MAN.001	
	MANUAL DE ORGANIZACIÓN Y FUNCIONES	Fecha: 16/04/2021	Versión: 1

Versión	1	Fecha de actualización	5/10/2021
Posición	**Practicante de Procesos (SIG)**		
Área	Proyectos		
Jefe Inmediato	Business Partner	Personal a cargo	No aplica
Objetivo de puesto	Apoyar en la implementación Seguridad y Salud en el Trabajo, Seguridad de la Información y otros sistemas que la organización desee optar. Apoyar en el mantenimiento del sistema de gestión de calidad y otros sistemas que la organización desee optar. Controlar los indicadores de todos los procesos de la organización e indicadores del sistema integrado de gestión.		
Funciones y responsabilidades principales	• Apoyar en el mantenimiento del sistema integrado de gestión y otros sistemas que la organización desee optar. • Apoyar en la gestión de riesgos y oportunidades de la empresa. • Revisar periódicamente el cumplimiento de los objetivos del Sistema Integrado de Gestión. • Apoyar en la gestión del plan de auditorías internas y externas de la empresa. • Medir la satisfacción del cliente y asegurarse el levantamiento de las desviaciones encontradas en la calidad de los productos servidos. • Gestionar los cambios de los procesos del sistema de gestión. • Apoyar en el seguimiento de las acciones para las oportunidades de mejora y para prevenir la aparición de no conformidades. • Cumplir con las medidas de prevención relacionados a seguridad y salud en el trabajo y seguridad de la información establecidas por el cliente. • Cumplir con los lineamientos del Sistema Integrado de Gestión (Calidad, Seguridad de la información, y Seguridad y Salud en el Trabajo) de la organización. • Concientizarse con la Política de Excelencia Organizacional. • Apoyar en la gestión de los riesgos de seguridad y salud en el trabajo, calidad y Seguridad de la información. • Coodinar las reuniones de Comites internos de la organización. • Coordinar las reuniones de revisión por la dirección y dar seguimiento a los acuerdos. • Cumplir con las políticas SI • Dar seguimiento al cumplimiento de las políticas SI		
Experiencia	6 meses		
Educación	Egresado o Bachiller de Sistemas, Ambiental, Industrial o afines.		
Conocimientos Específicos (Formación)	Deseable Especialización en Gestión de Calidad, Seguridad, Medio Ambiente, Sistemas Integrados de Gestión, Procesos.		
Habilidades	•Pensamiento analítico •Eficiencia •Puntualidad •Asertividad •Comunicación		

Figura 22

Manual de organización y funciones

Core Business Corp.	MANUAL	Código: MAN.001	
	MANUAL DE ORGANIZACIÓN Y FUNCIONES	Fecha: 16/04/2021	Versión: 1

Versión	1	Fecha de actualización	16/04/2021
Posición	**Business Partner**		
Área	Proyectos		
Jefe Inmediato	Socio Principal	Personal a cargo	• Consultores • Terceros
Objetivo de puesto	Supervisar y dar soporte en la ejecución de planes de proyectos por cliente de Core Business Corp. Realizar la gestión de proveedores. Conforma la Alta Dirección		
Funciones y responsabilidades principales	**Gestión de Proveedores** •Gestionar el reclutamiento de los proveedores. •Evaluar periódicamente a los proveedores los cuales brindan nuestros servicios. •Capacitar a los proveedores con relación a los lineamientos de CBC. •Revisar los entregables de los proveedores. Asegurar el cumplimiento de las necesidades especificadas del Consultor Líder y/o cliente. **Planes de Proyectos** •Proveer los recursos necesarios (personal) para el cumplimiento de los planes cada proyecto • Apoyar el cumplimiento de los planes de proyecto. •Cumplir con las medidas de prevención relacionados a Seguridad y Salud en el Trabajo establecidas y Seguridad de Información por el cliente. •Cumplir con los lineamientos del Sistema Integrado de Gestión (Calidad, Seguridad de la información, y Seguridad y Salud en el Trabajo) de la organización. • Concientizarse con la Política de Excelencia Organizacional y Políticas SI • Cumplir con la Política de Excelencia Organizacional y Políticas SI		
Experiencia	Experiencia mínima de 5 años (Obligatorio)		
Educación	Titulado en Ingeniería: Sistemas, Ambiental, Industrial o afines. (Obligatorio) MBA, Maestría en Seguridad y Salud en el Trabajo, Maestría en Sistemas de gestión o afines (Deseable)		
Conocimientos Específicos (Formación)	• Auditor Líder ISO 45001 o OHSAS 18001. (Obligatorio) • Diplomado de Prevención de Riesgos laborales. (Obligatorio) • Especializacón en Gestión de Calidad ISO 9001 (Obligatorio) • Prevención de COVID 19 (Obligatorio) • Auditor Líder ISO 9001. (Deseable) • Auditor Líder ISO 27001. (Deseable)		
Habilidades	• Negociación • Servicio al cliente • Asertividad • Comunicación • Flexibilidad		

VI.15. ANEXO 13. Rendición de cuentas

Figura 23

Rendición de cuentas

Core Business Corp.	POLÍTICA	Código: POL.009	
	RENDICIÓN DE CUENTAS	Fecha: 24/05/2021	Versión: 2

N°	Cargo	Nombre	Rendición de cuentas	Tema relacionados a la rendición	Autoridad
1	Socio Principal / Accionista Principal	Dante Velasquez	Entidades del estado Clientes (Legal)	Rinde cuentas en temas legales a los clientes, entidades del estado, otros. Rinde cuentas de la gestión comercial hacia las partes interesadas. Aprueba los planes estratégicos de la organización	Máxima autoridad de CBC
2	Oficial de SI	Paul Aliaga	Socio Principal	Rinde cuenta de la implementación del Sistema de Gestión de Seguridad de la información. Acorde al Plan de SI y tema legal.	Representante en la empresa para temas de SI
3	Coordinador de Desarrollo Procesos	Lucero Arana	Socio Principal	Rinde cuentas de la implementación del Sistema Integrado de Gestión cumple con la ISO 9001. Revisa y controlar el aseguramiento que los procesos están generando y proporcionando las salidas previstas; Rinde cuentas sobre el desempeño del SGC y sobre las oportunidades de mejora, mediante la Revisión por la Dirección. Se asegura que se promueve el enfoque al cliente en toda la organización; Rinde cuentas de la planificación, seguimiento de la implementación de los cambios que aseguren la integridad del SIG.	Representante en la empresa para temas del Sistema de Gestión de Calidad, acorde a la ISO 9001
4	Consultor Líder	Isabel Huapaya, Mirella Aucapiña	Socio Principal.	Rinde cuenta del cumplimiento de los planes de los entregables con los clientes, así como de su satisfacción.	Responsable de la gestión de los proyectos con los clientes.
5	Jefe de Administración y Finanzas	Solange Nieto	Socio Principal	Rinde cuentas del control económico y financiero de la organización. Rinde cuentas de los procesos de comunicación y capacitación interna.	Responsable de la gestión de recursos financieros y gestión de recursos humanos.

VI.16. ANEXO 14. Alcance

Figura 24

Alcance

	POLÍTICA	Código: POL.003	
Core Business Corp	ALCANCE DEL SISTEMA INTEGRADO DE GESTIÓN	Fecha: 24/05/2021	Versión: 3
		Página 1 de 3	

1. OBJETIVO

El presente documento establece el alcance del Sistema Integrado de Gestión de Core Business Corporation.

2. ALCANCE

El presente Sistema Integrado de Gestión alcanza a los servicios de:

- Provisión de Servicios de Consultoría de Sistemas de Gestión.
- Capacitación (incluido e-learning)
- Auditorías.

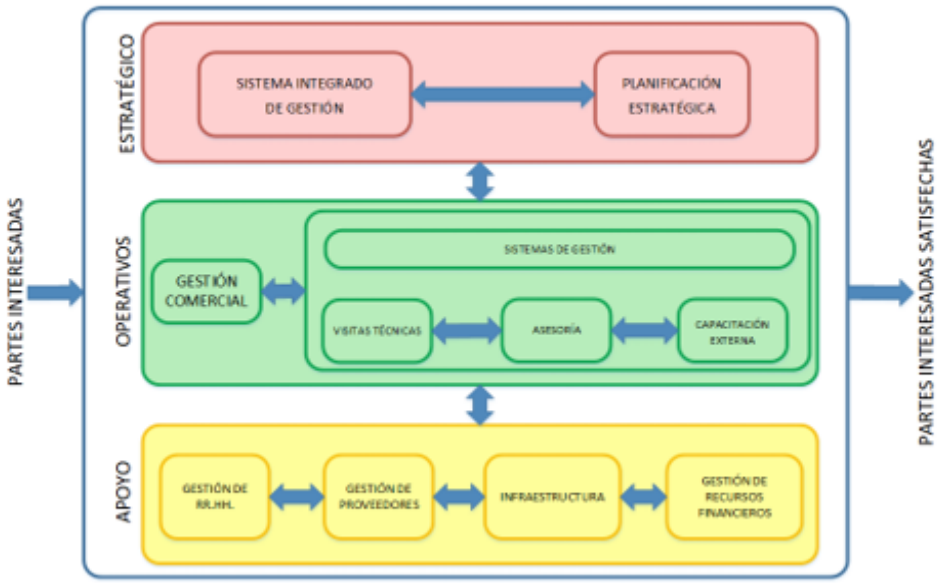
Los siguientes requisitos de la norma ISO 9001:2015 no son aplicables a nuestro Sistema Integrado de Gestión:

- 8.3 Diseño y desarrollo de los productos servicios. Sustento: Al ser la CBC, una empresa encargada de brindar servicios, no se dedica al diseño y desarrollo, ya que no gestionamos procesos que transforman los requisitos de un servicio de capacitación, auditorías y asesorías.
- 8.5.1 f) la validación y revalidación periódica de la capacidad para alcanzar los resultados planificados de los procesos de producción y de prestación del servicio, cuando las salidas resultantes no puedan verificarse mediante actividades de seguimiento o medición posteriores. Sustento: Al ser una empresa de consultoría de asesorías, capacitaciones, auditorías de sistemas de gestión, nuestro servicio es puntual. No se puede confirmar, mediante evidencia objetiva, de que se han cumplido, con anterioridad, los requisitos del servicio.

Para el caso de la ISO 27001:2013 se determina los límites y aplicabilidad del sistema de gestión de seguridad de la información en el FOR.064 Aplicabilidad.

3. LIMITES Y APLICABILIDAD

Mapa de Procesos



VI.17. ANEXO 15. Procedimiento de Gestión de riesgos y oportunidades

Figura 25

Procedimiento de Gestión de riesgos y oportunidades

	PROCEDIMIENTO	Código: PRO.005	
Core Business Corp.	GESTIÓN DE RIESGOS Y OPORTUNIDADES	Fecha: 05/10/2021	Versión: 4
		Página 1 de 6	

1. OBJETIVO

Establecer la metodología para la identificación de amenazas, oportunidades, evaluación de riesgos y determinar los controles necesarios para eliminar los riesgos o reducir su impacto; asimismo, definir los controles que logren el mejor impacto en las oportunidades identificadas.

2. ALCANCE

Aplica a todos los procesos relacionados con el SIG.
Para temas de Seguridad y Salud en el trabajo, se considera los riesgos y oportunidades hacia los procesos que afecten a la salud de los trabajadores. No está considerado el análisis técnico de peligros, riesgos hacia la prevención de accidentes y enfermedades profesionales.
Para temas de Seguridad de la información, se considera los riesgos y oportunidades hacia los procesos que afecten a los activos de información.

3. REFERENCIAS:

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Seguridad de la Información.

5. DESARROLLO

5.1. Identificación y análisis de riesgos y oportunidades del contexto de la organización

El Socio Principal identifica los riesgos y oportunidades a nivel estratégico establecido en el **FOR.015 - Análisis de Contexto y Partes interesadas**. El análisis es la determinación de cuestiones internas (fortalezas y debilidades) y externas (oportunidades y amenazas), partes interesadas que son pertinentes a la estrategia al SIG.

Las estrategias identificadas en el Plan Estratégico y las partes interesadas son consideradas en el análisis de riesgos.
Para el caso de los activos de información se identificara los

5.2. Elaboración de matriz de riesgos y oportunidades de procesos

5.2.1. Identificación y análisis de riesgos y oportunidades

El jefe de administración y Finanzas, Business Partner y el Consultor Líder son responsables de la identificación de riesgos y oportunidades de sus procesos en el formato: **FOR.013. Matriz de identificación de riesgos y oportunidades**
Se aborda con el fin de:

- Asegurar que el sistema integrado de gestión pueda lograr sus resultados previstos.
- Aumentar los efectos deseables.
- Prevenir o reducir efectos no deseados.
- Lograr la mejora.

5.2.2. Evaluación y valoración de riesgos y oportunidades identificados

El jefe de administración y Finanzas, Business Partner y el Consultor Líder evalúan y valoran los riesgos y oportunidades identificadas según el Anexo 1 – Evaluación y valoración de Riesgos y Oportunidades.
Realiza el análisis de riesgos y oportunidades de acuerdo con los tipos de riesgos y oportunidades (Ver Anexo 2).

VI.18. ANEXO 16. Procedimiento de Gestión de activos

Figura 26

Procedimiento de Gestión de Activos

	PROCEDIMIENTO	Código: PRO.025	
Core Business	GESTIÓN DE ACTIVOS	Fecha: 08/03/2021	Versión: 1
		Página 1 de 5	

1. OBJETIVO

El presente documento establece los lineamientos a seguir para establecer, mantener y asegurar un nivel de protección adecuado para los activos de información de Core Business Corporation.

2. ALCANCE

Aplica a todo el personal de CORE BUSINESS CORPORATION.

3. REFERENCIAS:

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. DEFINICIONES

- **Activo de información:** Es todo aquello que representa valor para la CBC desde software, hardware, información, servicios y colaboradores.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Propietario del activo:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Usuario:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

5. RESPONSABILIDADES

5.1. Oficial de Seguridad de la Información

- Informar al Socio principal sobre el desempeño del SGSI.
- Dar seguimiento a los registros de SGSI.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Promover la capacitación y concientización de los colaboradores acerca de la gestión de la seguridad de la información.
- Liderar los proyectos de mejora del SGSI.

5.2. Propietario del Activo de Información

- Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- Entender y abordar los riesgos relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

5.3. Usuario del Activo de Información

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.

VI.19. ANEXO 17. Procedimiento de Gestión de riesgos SI

Figura 27

Gestión de riesgos operacionales de SI

	PROCEDIMIENTO	Código: PRO.023	
Core Business Corp	GESTIÓN DE RIESGOS OPERACIONALES	Fecha: 5/10/21	Versión: 1
		Página 1 de 5	

1. **OBJETIVO**

Establecer el proceso para la identificación, análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información; asimismo, definir los controles que permitan mitigar o disminuir el riesgo identificados.

2. **ALCANCE**

Aplica a todos los procesos relacionados con el SIG.

Se considera los riesgos y oportunidades hacia los procesos que afecten a los activos de información.

3. **REFERENCIAS:**

- ISO 27001:2013. Requisitos de un Sistema de Seguridad de la Información.
- ISO 27002. Técnicas de seguridad Código de prácticas para los controles de seguridad de la información.
- ISO 3100. Gestión de Riesgos

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Riesgo aceptable:** es el riesgo que se ha conseguido reducir o mitigar de tal forma que pueda ser tolerado por la organización. Nivel de riesgo medio o bajo.
- **Riesgo residual:** riesgo restante después del tratamiento del riesgo.
- **Probabilidad:** Posibilidad de que el evento riesgoso ocurra de acuerdo con situaciones ya presentadas basadas en registros reales, datos, hechos o información conocida.
- **Amenaza:** Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática.
- **Impacto:** Consecuencia que pueda ocasionar en la empresa la materialización del riesgo.
- **Propietario:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Custodio:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Vulnerabilidad:** Debilidad de los sistemas, ya sean equipos de cómputo, servidores, tanto hardware como software, sistema operativo, sistemas de información, aplicaciones, redes, etc. que puede ser utilizados o aprovechados por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.
- **Consecuencia:** el resultado de un evento (amenaza) que afecta a los objetivos.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

VI.20. ANEXO 18. Procedimiento de G.RRHH

Figura 28

Gestión de RRHH

	PROCEDIMIENTO	Código: PRO.009	
Core Business Corp.	GESTIÓN DE R.R.H.H	Fecha: 24/11/2021	Versión: 4
		Página 1 de 5	

1. OBJETIVO

Establecer los lineamientos para gestión de los recursos humanos de Core Business Corp. (CBC), desde el ingreso de los nuevos colaboradores, los procesos de formación, conocimientos de la empresa; la observación, medición y análisis del desempeño laboral y la desvinculación de los colaboradores de CBC.

Reconocer al colaborador que mediante el despliegue de sus conocimientos, habilidades y actitudes alcanza un extraordinario desempeño organizacional

2. ALCANCE

Este procedimiento es de alcance a todos los trabajadores de Core Business Corp (CBC).

3. REFERENCIAS

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO/IEC 27001: 2013 Gestión de seguridad de la información

4. DEFINICIONES

- **Competencia:** capacidad con la que se aplican los conocimientos y las habilidades con el fin de conseguir los resultados previstos.
- **Retroalimentación o Feedback:** Proceso de retroalimentación en el cuál intervienen un colaborador y su jefe con la finalidad de establecer un plan de mejora que impacte positivamente en los factores que afectan el desempeño.
- **Formación:** Es un proceso de mejora continua en el que se busca mejorar las habilidades personales y laborales, así como aumentar la productividad de los colaboradores. Asimismo, permite la reducción de accidentes de trabajo debido a la implementación de conocimientos y la satisfacción laboral.
- **Capacitación:** Es el proceso destinado a promover, facilitar, fomentar y desarrollar las aptitudes, habilidades o grados de conocimiento de los trabajadores, con el fin de permitirles mejores oportunidades, condiciones de vida y de trabajo, y de incrementar la productividad procurando la necesaria adaptación de los trabajadores a los procesos tecnológicos y a las modificaciones estructurales de la economía.

5. DESARROLLO

5.1 Reclutamiento y selección

El proceso de reclutamiento y selección es realizado por el Practicante de Psicología laboral, bajo la supervisión del Jefe de Administración y Finanzas.

Las actividades de reclutamiento y selección consideran el perfil de puesto descrito en el Manual de Organización y funciones de la Organización.

La actividad de reclutamiento se realiza a través de la publicación en bolsa de trabajo y solicitud, mediante correo electrónico, de recomendaciones al personal de CBC.

La selección del nuevo trabajador se realiza en las siguientes etapas:

- Evaluación preliminar de la hoja de vida de los postulantes; debe cumplir con lo establecido en el perfil de puesto.
- Confirmación de las referencias y veracidad del Currículo de los postulantes.
- Entrevista personal o virtual, a cargo del Practicante de Psicología Organizacional, Jefe del Área y Socio Principal.
- Evaluación de capacidades, se envía una actividad relacionada al puesto de trabajo para que sea desarrollada por el postulante, de acuerdo con el resultado de esta actividad se define al postulante seleccionado.
- Solicitud y revisión de antecedentes policiales, judiciales y penales del candidato seleccionado
- Comunicación a los postulantes, seleccionados y no seleccionados el fin del proceso.

Todos los postulantes pasan por todas las etapas de selección hasta llegar a la evaluación final, si el postulante no cumple los requerimientos de una etapa, se descalifica.

VI.21. ANEXO 19. FOR.018 Evaluación del desempeño

Figura 29

Evaluación del desempeño

Core Business Corp.	FORMATO	Código: FOR. 018	
	EVALUACIÓN DE DESEMPEÑO	Fecha: 08/03/2021	Versión: 2

Fecha de evaluación
Nombre del evaluado
Cargo del evaluado

Nombre del evaluador Dante Velasquez
Cargo del evaluador Socio Principal

	Valor	Nivel	Descripción
Los valores a considerar en la calificación de competencias son los siguientes:	4	SOBRESALIENTE	Dominio sobresaliente de la competencia.
	3	LOGRADO	Se observa con bastante frecuencia pero no siempre. Está en un buen nivel de desempeño.
	2	CUMPLE PARCIALMENTE	La competencia se muestra en un nivel inicial, está en desarrollo.
	1	NO CUMPLE	No se observa la competencia o se presenta muy poco. Aun no logra desplegar este aspecto.

GRUPO DE COMPETENCIAS	COMPETEN CIAS	DEFINICIÓN	EJEMPLOS	VALOR
ENTORNO	Adaptabilidad a diferentes entornos	Mantiene un buen nivel de desempeño independientemente de las circunstancias, ambientes de trabajo, jefes, clientes, proveedores o equipos de trabajo.	Se adecua a los cambios del cliente, a las nuevas formas de trabajo (teletrabajo, plataformas).	
	Trabajo en equipo	Se integra fácilmente al equipo de trabajo y se enfoca en el cumplimiento de los objetivos de equipo. Asimismo, se comunica de manera asertiva con actitud positiva.	Apoya a los miembros del equipo, brinda soluciones rápidas y de manera efectiva.	
CLIENTE	Conocimiento técnico	Conoce y está al tanto de las normativas, procedimientos relacionados a la consultoría de la empresa y del área asignada. Aplica los procedimientos permanentemente.	Conocimientos de leyes y normativas de SST.	
	Relación con clientes externos e internos	Identifica y satisface las necesidades de los clientes externos e internos. Promueve efectivamente relaciones de cooperación y confianza a largo plazo. Conoce y respeta los procedimientos de sus clientes, a fin de evitar obstaculizar los procesos. Muestra una comunicación asertiva, presenta estrategias innovadoras adecuadas al cliente y muestra una actitud positiva.	Muestra un trato respetuoso hacia los clientes, es tolerante y comprensivo/a.	
	Puntualidad	Llega a tiempo según la hora pactada a: reuniones de trabajo, dictar capacitaciones, auditorías y a otras labores propias de los servicios brindados por CBC. Presenta entregables en la fecha estimada por los medios correspondientes.	Llega a la hora acordada a las reunión con clientes internos y externos.	
	Resolución de problemas	Encuentra soluciones buscando diferentes alternativas ante las adversidades, evitando caer en inacción.	Manejo de conflictos con el cliente, solución a problemas diarios en el trabajo	
	Calidad de trabajo	Presenta informes, entregables, documentos con la calidad respectiva, basada en evidencia, leyes y normativas. Asimismo, presenta redacción y ortografía correcta. Afán por mejorar continuamente y superar los estándares requeridos en su trabajo, logrando cumplir, e incluso elevar, la calidad de las tareas encomendadas.	Informes de SST basados en la ley 29783.	
PROCESOS INTERNOS	Proactividad: Alternativas de mejora	Comparte su conocimiento de manera proactiva y desinteresada. Por iniciativa propia, busca y pregunta dentro y fuera de la organización para adquirir el conocimiento requerido para desempeñar sus funciones y superar obstáculos. Presenta una mejora de procesos y aportes novedosos a la organización.	Aplica una adecuada respuesta estratégica en un nuevo proyecto, en la mejora de procesos que afecta directamente los encargos que se le han encomendado.	
	Eficiencia	Prioriza y promueve el bien de la empresa o por encima del beneficio del encargo encomendado. Comparte desinteresadamente recursos propios en beneficio de CBC. Realiza sus funciones y responsabilidades en un tiempo esperado. Busca la opción más óptima que brinde mayores beneficios a la empresa.	Utiliza adecuadamente los recursos de la empresas, búsqueda del ahorro en la empresa.	
			PROMEDIO TOTAL	#¡DIV/0!

COMPROMISOS		
DESCRIPCIÓN DEL COMPROMISO	FECHA DEL CUMPLIMIENTO	RESPONSABLE

Firma del colaborador

Firma del evaluador
Dante Velasquez

VI.22. ANEXO 20. PRO.008 Capacitación

Figura 30

Procedimiento de Capacitación

	PROCEDIMIENTO	Código: PRO.008	
Core Business Corp	CAPACITACIÓN	Fecha: 25/05/2021	Versión: 3
		Página 1 de 3	

1. OBJETIVO

Garantizar la formación y competitividad de nuestros colaboradores mediante la capacitación en modalidad presencial y/o virtual, con los siguientes fines:

- Lograr el óptimo desempeño de las funciones de los colaboradores.
- Mantener a los colaboradores actualizados.
- Ser referentes técnicos en diversos temas en los que la empresa ofrece sus servicios.
- Prevenir accidentes y enfermedades profesionales aplicable a todos.

2. ALCANCE

El presente procedimiento es aplicable a todos los colaboradores de Core Business Corporation (CBC).

3. REFERENCIAS

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013: Requisitos de un Sistema de Seguridad de la información

4. DEFINICIONES

- **Formación:** Es un proceso de mejora continua en el que se busca mejorar las habilidades personales y laborales, así como aumentar la productividad de los colaboradores. Asimismo, permite la reducción de accidentes de trabajo debido a la implementación de conocimientos y la satisfacción laboral.
- **Capacitación Interna:** Es aquella que se da únicamente a los trabajadores de CBC.
- **Capacitación Externa:** Es aquella que a la que puede asistir personas ajenas a la empresa, además de los trabajadores de CBC.
- **Capacitación Individual:** Este tipo de capacitación tiene una duración que varía, puede ser de horas o, incluso, de meses. Puede ser impartida por medio de cursos, seminarios, talleres, instituciones educativas, entre otras formas. Se programa de acuerdo con las necesidades de cada persona o de los grupos de trabajo para que adquieran las habilidades y el conocimiento que requieran aplicar en su beneficio y el de la compañía.
- **Capacitación General:** Es aquella que se brinda a todo el personal de CBC.

VI.23. ANEXO 21. Comunicaciones

Figura 31

Comunicaciones SI

Figura 31

Comunicaciones SI

Figura 31

Comunicaciones SI

Figura 31

Comunicaciones

Figura 31

Comunicaciones

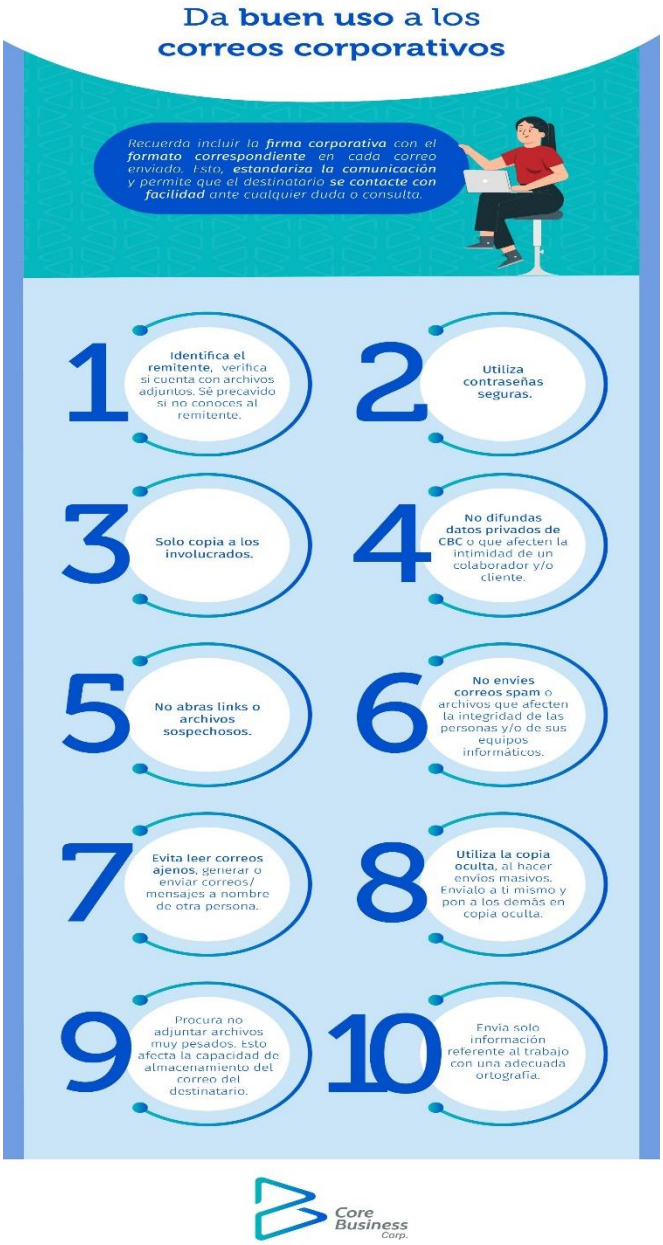


Figura 31

Comunicaciones

VI.24. ANEXO 22. PRO.001 Control de información documentada

Figura 32

Procedimiento de Control de información documentada

	PROCEDIMIENTO	Código: PRO.001	
Core Business Corp.	CONTROL DE INFORMACIÓN DOCUMENTADA	Fecha: 14/05/2021	Versión: 2
		Página 1 de 5	

1. **OBJETIVO**

Establecer la metodología y responsabilidades para elaborar, distribuir, acceder controlar, disponer, almacenar, preservar y recuperar la información del Sistema Integrado de Gestión.

2. **ALCANCE**

Aplica a todos los procesos y documentos relacionados con el Sistema Integrado de Gestión.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la Información

4. **DEFINICIONES**

- **Copia controlada:** Copia de un documento distribuido por la organización, del cual debe asegurarse que se use la última versión.
- **Documento externo:** Documento recibido de una tercera parte, entre quienes están cliente, proveedor, entidades, etc.
- **Documento interno:** Documento generado internamente en la organización para el desarrollo de sus actividades.
- **Documento obsoleto:** Documento no actualizado el cual se encuentra como no vigente.
- **Lista maestra de información documentada:** Registro de la relación de todos los documentos utilizados en la organización, el cual permite identificar los registros relacionados a los documentos, el tiempo de retención, tipo de almacenamiento e identificar el nombre del usuario responsable y el número de versión de cada documento distribuido.
- **Procedimiento:** Forma específica para llevar a cabo una actividad o un proceso.

5. **CONSIDERACIONES GENERALES**

Para todos los documentos externos del cliente, CBC se asegura de la confidencialidad de la información entregada, para fines solo de consulta mientras se ejecuta el servicio puntual. Por ende, CBC no registra dichos documentos en la Lista Maestra de Información Documentada.

6. **DESARROLLO**

6.1. Elaboración y/o actualización

Todo colaborador puede elaborar un documento interno para ser incluido al Sistema Integrado de Gestión (SIG), el cual es revisado y aprobado por las áreas responsables, y debe mantener el formato y estructura establecidos en el anexo 1. Al finalizar la elaboración, el colaborador debe enviar el documento al responsable de desarrollo de proceso SIG.

En caso de que el colaborador solicite un cambio en los documentos, debe emitir un correo al responsable de desarrollo de proceso SIG.

VI.25. ANEXO 23. PRO.004 Gestión de cambio

Figura 33

Procedimiento de Gestión de Cambio

	PROCEDIMIENTO	Código: PRO.004	
Core Business Corp	GESTIÓN DEL CAMBIO	Fecha: 14/05/2021	Versión: 2
		Página 1 de 2	

1. **OBJETIVO**

El presente documento establece los lineamientos para gestionar los cambios, procesos de negocio, instalaciones de procedimiento de la información y sistemas, y las modificaciones que impactan al Sistema Integrado de Gestión.

2. **ALCANCE**

Aplica a todos los cambios mayores relacionados con el Sistema Integrado de Gestión.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Requisitos de un Sistema de gestión de seguridad y salud en el trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la Información.

4. **DEFINICIONES**

- **SIG:** Sistema Integrado de Gestión.
- **Cambio mayor:** Cambio que involucra la intervención de la gerencia, tal y como lo muestra la tabla 1.
- **Cambio menor:** Cambios que pueden ser gestionados por acciones correctivas y no implica la necesidad gestionar un proyecto detallado, por ejemplo: control de cambios en la información documentada, cambios de fecha, auditor, lugar de ejecución, etc., de los servicios coordinados con el cliente.

5. **DESARROLLO**

5.1. **Identificación de necesidad de cambio**

Todo colaborador de CBC puede identificar y generar una solicitud de cambio. Dicha solicitud será considerada siempre y cuando se exponga un cambio que afecte al SIG, como lo expone la tabla 1.

Tabla 1. Listado de cambios aplicables

Estratégico	• Cambio de planificación estratégica (análisis de contexto). • Aspectos legales.
Financieros	• Asignación o reasignación de presupuesto a alguna área específica o por algún requerimiento específico. • Compra de servicios o bienes mayores a 15000 soles.
Recurso Humano	• Asignación o reasignación de responsabilidades. • Creación de nuevos puestos de trabajo.
Procesos Operativos	• Cambio de metodología de auditoria, inspección, asesoría, capacitación. • Adición de nuevos servicios.
Procesos de Apoyo	• Cambio de infraestructura tecnológica a nivel corporativo. • Cambio de ambiente de trabajo.

Tras la identificación, el colaborador debe comunicarlo enviando un correo al responsable de Desarrollo de Procesos y Socio Principal para su respectiva evaluación.

VI.26. ANEXO 24. PRO.015 Infraestructura Tecnológica

Figura 34

Procedimiento Infraestructura Tecnológica

	PROCEDIMIENTO	Código: PRO.015	
Core Business	INFRAESTRUCTURA TECNOLOGICA	Fecha: 08/03/2021	Versión: 1
		Página 1 de 3	

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para elaborar y controlar los documentos relacionados a los servicios informáticos de Core Business Corporation.

2. **ALCANCE**

Aplica a todos los procedimientos y documentos relacionados con el Sistema Integrado de Gestión de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001: Sistema de Gestión de Seguridad de la Información.

4. **DEFINICIONES**

- **CPanel:** Permite administrar una cuenta de alojamiento web con la máxima eficiencia. Ya sea creando nuevos usuarios FTP y direcciones de correo electrónico o monitoreando recursos, creando subdominios e instalando software.
- **Hosting:** Es un servicio de alojamiento para sitios web. El hosting web aloja los contenidos de tu web y tu correo electrónico para que puedan ser visitados en todo momento desde cualquier dispositivo conectado a Internet.
- **Dominio:** Un dominio web es el nombre único que recibe un sitio web en internet. Este nombre identifica a una página web concreta sin que puedan existir dos o más sitios web que compartan el mismo nombre de dominio.
- **Backup de Información:** Es una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Antivirus:** Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Una vez instalados, la mayoría del software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus.

5. **DESARROLLO**

5.1. Gestor de Hosting Dominio y Correo Electrónico:

El Coordinador de Hosting, Dominio y Correos realiza el servicio de mantenimiento, monitoreo del hosting y dominio, backup de información en el hosting.

Valida el requerimiento de la solicitud de correo en el **FOR.035 Formato de información de personal nuevo y entrega de equipo.**

Crea nuevo correo en el cpanel según lo detallado en el documento INS.003 – Creación de nuevo correo en CPANEL

Configura correo electrónico en el equipo del usuario.

Configura y archiva de correos, creación de carpeta pst en el equipo del usuario.

Realiza baja de correos, según instructivo INS.008 – Eliminación de Correo

Realiza backup de correos desde Webmail, según instructivo INS.004 – Backup de Correo

Realiza mantenimiento buzón de correos en servidor, según instructivo INS.009 – Mantenimiento de buzón de correos en el servidor.

5.2. Gestor de Soporte Técnico:

El Coordinador de Hosting, Dominio y Correos atiende a las consultas de apoyo de los clientes

Administra software y herramientas de asistencia técnica.

Realiza diagnóstico y solución de problemas de los clientes.

Está pendiente de la actualización de los productos y servicios de la empresa.

Realiza instalación y configuración de equipos de cómputo.

Realiza mantenimiento Preventivo de equipos de cómputo, según instructivo INS.005 – Mantenimiento preventivo de equipo de cómputo.

Registra y Controla Compromisos de Seguridad de la Información a los usuarios, según instructivo FOR.036– Compromiso de seguridad de la información.

VI.27. ANEXO 25. PRO.003 Gestión de auditoria

Figura 35

Procedimiento de Gestión de Auditoria

	PROCEDIMIENTO	Código: PRO.003	
Core Business	GESTIÓN DE AUDITORIA	Fecha: 16/09/2021	Versión: 4
		Página 1 de 3	

1. **OBJETIVO**

Establecer el procedimiento para la planificación, programación y realización de las auditorías internas, con la finalidad de evaluar si el Sistema Integrado de Gestión se ha implementado y se desarrolla de manera eficaz.

2. **ALCANCE**

Este procedimiento aplica al Sistema Integrado de Gestión.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la Información

4. **DEFINICIONES**

- **SIG:** Sistema Integrado de Gestión.
- **Auditoría Interna:** Auditoría realizada por miembros de la propia organización o por otras personas que actúan de parte de ésta, para fines internos.
- **Auditoría Externa:** Se realiza por una organización externa, independiente y autorizada con el objeto principal de obtener una certificación del sistema de gestión de calidad, el cual puede presentarse a los clientes potenciales y proveedores aumentado la confianza en la organización.
- **Conformidad:** Cumplimiento de un requisito.
- **Criterios de Auditoría:** Conjunto de políticas, procedimientos o requisitos utilizados como referencia.
- **Evidencia de la Auditoría:** Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables. La evidencia del auditor puede ser cualitativa o cuantitativa.
- **Hallazgo de la Auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.
- **No Conformidad:** Incumplimiento de un requisito especificado.

5. **DESARROLLO**

5.1. Planificación

El responsable de desarrollo de proceso SIG y Business Partner en conjunto con el Socio Principal elabora el **FOR.009 - Programa Anual de Auditorías**, para ello se debe tener en cuenta los siguientes aspectos:

- Se deben auditar todos los procesos de la organización y requisitos de las normas ISO 9001:2015, ISO 45001:2018 e ISO 27001:2013, por lo menos una vez al año.
- Definir los criterios y el alcance de cada auditoría mediante **FOR.010 Plan de Auditoria**;
- Seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría; El Business Partner designa el responsable de la auditoria, cuyo proceso de contratación sigue los lineamientos del procedimiento **PRO.011 - Gestión de Proveedores**. El Auditor líder deberá ser profesional universitario, además deberá contar como mínimo con experiencia de 10 años en auditorías que sean demostrables mediante certificado de trabajo.

  Para el caso se la ley 29783, los requisitos son los siguientes:
  -De ser el caso estar acreditado como Auditor de SST en el MINTRA.

  -Haber realizado por lo menos 5 auditorías de SST.
- Asegurar que los resultados de las auditorías se reporten a los gerentes de acuerdo a los lineamientos del **PRO. 007 revisión por la Dirección**, y se informen los hallazgos a los trabajadores, a los representantes de trabajadores y a otras partes interesadas relevantes; y
- Resultados de auditorías previas.
- Tomar acciones para abordar los Reclamos de clientes, no conformidades y acciones correctivas registradas en el **FOR.007 Base de Datos de AC siguiendo el** PRO.002 Tratamiento de No Conformidad y Acciones Correctivas
- Retener información documentada como evidencia del (de los) programa(s) de auditoría y los resultados de la auditoría.

El programa de auditoria se revisa en conjunto con el Socio Principal y se aprueba según sea conveniente, ya sea en una reunión o por correo electrónico.

VI.28. ANEXO 26. FOR.009 Programa anual de auditoria

Figura 36

Programa de auditoria 27001:2013

	FORMATO	Código: FOR.009	
	PROGRAMA ANUAL DE AUDITORIAS	Fecha: 14/05/2021	Versión: 4

TIPO AUDITORIA	N° de Auditorias	Alcance	Objetivo	Responsable	Criterios	Métodos	Riesgos	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar
Auditoria Interna	1	Todas las actividades de CBC	Cumplimiento de la ISO 9001:2015	José Luis Sandoval	ISO 27001:2013 ISO 9001:2015 ISO 45001:2017	virtual (Microsoft Teams).	**Riesgos en la planificación:** -Mala coordinación para definir las fechas de las auditorías de acuerdo a la disponibilidad del personal clave del auditado. **Riesgos en los recursos:** -Fallas en la conexión en caso de auditorías virtuales (trabajo remoto). -No contar con recurso financiero suficiente. **Riesgos asociados al equipo de auditores:** -No contar con auditores calificados y con las competencias necesarias. **Riesgos en la implementación:** -Falta de preparación y conocimiento por parte del personal auditado para respuesta frente a una auditoría. -Falta de comunicación del área responsable hacia los colaboradores de la empresa sobre eventos de auditorías.												P			
Auditoria Externa	1	Todas las actividades de CBC	Certificacion de la ISO 27001:2013	Lloyds	ISO 27001:2013 ISO 45001:2018	virtual (Microsoft Teams).	**Riesgos en la planificación:** -Mala coordinación para definir las fechas de las auditorías de acuerdo a la disponibilidad del personal clave del auditado. **Riesgos en los recursos:** -Fallas en la conexión en caso de auditorías virtuales (trabajo remoto). -No contar con recurso financiero suficiente. **Riesgos asociados al equipo de auditores:** -No contar con auditores calificados y con las competencias necesarias. **Riesgos en la implementación:** -Falta de preparación y conocimiento por parte del personal auditado para respuesta frente a una auditoría. -Falta de comunicación del área responsable hacia los colaboradores de la empresa sobre eventos de auditorías.														P	

VI.29. ANEXO 27. PRO.011 Gestión de Proveedores

Figura 37

Gestión de proveedores

	PROCEDIMIENTO	Código: PRO.011	
Core Business Corp.	GESTIÓN DE PROVEEDORES	Fecha: 8/03/2021	Versión: 2
		Página 1 de 3	

1. OBJETIVO

El presente documento establece los lineamientos a seguir para la selección, evaluación, contratación y re-evaluación de proveedores, contratistas y contratación externa que presten servicios a Core Business Corp (CBC).

2. ALCANCE

Aplica a todos los proveedores que presten los servicios de capacitación externa, auditoría, inspecciones, asesorías y procesos internos.

3. REFERENCIAS:

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013: Sistema de Seguridad de la información.

4. DEFINICIONES

- **Proveedor interno**: Persona que presta servicios a los procesos internos de CBC.
- **Proveedor externo**: Persona que brindan servicios a los clientes a nombre de CBC.
- **Servicio interno**: Proyectos o servicio constante que un proveedor realiza a los procesos internos de CBC.

5. DESARROLLO

5.1. Análisis de necesidad de servicio

El Business Partner realiza el análisis de necesidad según proceso, actividad, servicio a brindar y nivel de criticidad, estas son:

Procesos Operativos - Actividad	Servicio	Criticidad
Capacitación	Interno, Tercerizado	Alto
Eco-Learning	Tercerizado	Alto
Auditorías	Interno, Tercerizado	Alto
Inspección	Interno, Tercerizado	Alto
Asesoría	Interno, Tercerizado	Alto

Procesos de Apoyo - Actividad	Servicio	Criticidad
Página web	Tercerizado	Medio
Contabilidad	Tercerizado	Medio

5.2. Búsqueda selección de proveedor

El Business Partner realiza la búsqueda de especialistas en el mercado, según perfil, necesidad del cliente y proyecto interno.

Solicita el curriculum documentado y/o declaración jurada. Selecciona a los proveedores de acuerdo con el cumplimiento del perfil de búsqueda.

ANEXO 28. PRO.007 Revisión por la dirección

Figura 38

Revisión por la dirección

	PROCEDIMIENTO	Código: PRO.007	
Core Business	REVISIÓN POR LA DIRECCIÓN	Fecha: 15/09/2021	Versión: 4
		Página 1 de 3	

1. **OBJETIVO**

Establecer los lineamientos para que la Alta Dirección revise a intervalos planificados el Sistema Integrado de Gestión y así asegurar continuamente su conveniencia, adecuación, eficacia, eficiencia y efectividad.

2. **ALCANCE**

Este procedimiento aplica a los procesos del Sistema Integrado de Gestión.

3. **REFERENCIAS**:

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Requisitos de un Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la Información.

5. DESARROLLO

5.1. Planificación de la Revisión por la dirección.

El responsable de desarrollo de proceso SIG planifica la actividad por lo menos una vez al año y/o cuando se estime conveniente de acuerdo a las necesidades de seguimiento y control del SIG, esta planificación debe estar presente en el **FOR.003 Programa SIG.**

El Socio Principal con apoyo del responsable de desarrollo de proceso SIG solicita la información necesaria para la revisión a los jefes de Áreas.

La información de entrada para la revisión por la dirección de calidad incluye:

- El estado de las acciones de las revisiones por la dirección previas (**FOR.004 Acta de comité)**
- Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la calidad. **(FOR.015 Análisis de Contexto)**
- La información sobre el desempeño y la eficacia del sistema de gestión de la calidad, incluida las tendencias relativas a:
  - La satisfacción del cliente y la retroalimentación de las partes interesadas pertinentes. **(PRO.006 Medición de satisfacción al Cliente)**
- El grado en que se han logrado los objetivos de la calidad. **(FOR.002 Objetivos e indicadores del SIG)**
  - El desempeño de los procesos y conformidad de los productos y servicios.
  - Las no conformidades y acciones correctivas. **(PRO.002 Tratamiento de No conformidad y AC)**
  - Los resultados de seguimiento y medición.
  - Los resultados de las auditorías. **(FOR.011 Informe de Auditoría si es el caso de una auditoría interna)**
  - El desempeño de los proveedores externos. **(FOR.019 Plantilla de evaluación de proveedores)**

VI.30. ANEXO 29. PRO.002 Tratamiento de NC y acción correctiva

Figura 39

Tratamiento de NC y AC

	PROCEDIMIENTO	Código: PRO.002	
Core Business	TRATAMIENTO DE NO CONFORMIDAD Y ACCIÓN CORRECTIVA	Fecha: 14/05/2021	Versión: 3
		Página 1 de 3	

1. OBJETIVO

Determinar la metodología para la ejecución de acciones correctivas, a fin de eliminar las causas que originan no conformidades que afectan al Sistema Integrado de Gestión (SIG).

2. ALCANCE

Este procedimiento aplica para la investigación de no conformidades y ejecución de acciones correctivas, y mejora continua del Sistema Integrado de Gestión (SIG).

3. REFERENCIAS:

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Sistema de Seguridad y Salud en el Trabajo.
- ISO27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la información.

4. DEFINICIONES

- **Conformidad**: Cumplimiento de un requisito.
- **Hallazgo de la Auditoría**: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

5. DESARROLLO

5.1. Identificación de no conformidades y/o oportunidades de mejora

El origen de las no conformidades puede venir de diversas fuentes:

- Reclamos de clientes
- Encuestas de satisfacción
- Verificación día por día
- Auditorías internas
- Auditorías externas
- Revisión por la dirección
- Comités de SIG
- Matriz de riesgos y oportunidades
- Objetivos del SIG
- No conformidades del servicio
- Matriz de análisis de riegos operativos SI

El tipo de hallazgo puede ser:

VI.31. ANEXO 30. FOR.007 Registro de Acciones correctiva

Figura 40

Registro de AC

	FORMATO	Código: FOR.007	
	REGISTRO Y SEGUIMIENTO DE LAS ACCIONES CORRECTIVAS	Fecha: 14/05/2021	Versión: 3

Actualización 1/10/2021

N° de Registro	N°	Fecha Registro	Sistema de Gestión	Fuente	Tipo de Hallazgo	Área Proceso	Descripción	Acción Correctiva	Responsable de ejecución	Recursos	Fecha Estimada	Fecha de Ejecucion	MES	Estado	%	Verificacion de la eficacia	Fecha de Cierre
4	8	9/04/2021	SGC	Revisión por la Dirección	Oportunidad de mejora	Sistema Integrado de Gestión	Tras la realización de la revisión por la dirección han salido acciones correctivas con relación a los puntos examinados: La necesidad de crear un repositorio exclusivo donde guardar la documentarión del SIG	Implementar mecanismos de automatización para el control de documentación Implementación de la ISO 2013:27001	LA	Laptop, personal humano	9/04/2021	20/11/2021	Noviembre	Ejecutado	100%		
	9				Oportunidad de mejora			.	CM	Laptop, personal humano	30/04/2021	30/04/2021	Abril	Ejecutado	100%		

VI.32. ANEXO 30. Verificación de Controles SI

Figura 41

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A2	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados. *Actualizar el FOR. 036 compromiso de Seguridad de la información *FOR.049 Compromiso de confidencialidad de los colaboradores. *compromiso de confidencialidad para el cliente(listado de personal)	Jefe administrativo/Socio Principal	23/08/2021	7/09/2021	**100%**	1	1	2	2	1.7	**BAJO**
	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. *Elaborar y comunicar/concientizar una política de control de acceso	Desarrollo de procesos/Business Partner	23/08/2021	12/09/2021	**100%**						
	Asegurar protección a los activos de la organización que son accesibles por los proveedores *Elaborar una política de proveedores *Contar con acuerdos	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**						
	*FOR.049 Compromiso de confidencialidad de los colaboradores	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.(nombrar las políticas)	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	1	1	1	1	1.0	**BAJO**

Figura 42

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A3	*Elaborar y comunicar/concientizar una política de control de acceso(licencias autorizadas, inventariar los equipos, cuando se renueva, código por computadora, antivirus con capacidades)	Analista Junior de Business Inteligente	23/08/2021	17/09/2021	**100%**	1	1	3	1	1.7	**BAJO**
	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios/TODOS LOS EQUIPOS CON ANTIVIRUS *Elaborar una política prohibiendo el uso de software no autorizado e implantación de controles que prevengan o detecten el uso de software no autorizado *Procedimiento de monitoreo de antivirus	Analista Junior de Business Inteligente	23/08/2021	17/09/2021	**100%**	1	1	3	1	1.7	**BAJO**
	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada. *Establecer una política de respaldo, y probar copias de información de software y del sistema.	Analista Junior de Business Inteligente	23/08/2021	17/09/2021	**100%**						
	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso *Concientizar con una política de control de acceso *Lista de perfil de usuario.(accesos a través d erales y perfiles/matriz - aplicaciones principales-roles-privilegios)	Analista Junior de Business Inteligente	23/08/2021	17/09/2021	**100%**	1	1	3	1	1.7	**BAJO**

Figura 43

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A4	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados. *Revisar y actualizar si es el caso los acuerdos, y comunicarlos a todos los colaboradores y proveedores.	Jefe administrativo/Socio Principal	23/08/2021	7/09/2021	**100%**	1	1	1	3	1.7	**BAJO**
A5	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada *Concientizar la protección del equipo con contraseñas seguras *Elaborar un comunicado sobre la seguridad en lugares públicos y protección del equipo con contraseñas seguras	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	2	3	1	1	3.3	**MEDIO**
	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa. *Elaborar un Plan de contingencia	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**						
	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades *Elaborar un procedimiento de gestión de incidentes (como se gestiona los incidentes-personas que reportan los incidentes(clientes-colaboradores);flujo de GI;GELDEX-gestor de incidentes/clasificando los incidentes crítico, medio, bajo.	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**						
	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada *Elaborar un comunicado sobre la seguridad en lugares públicos y protección del equipo con contraseñas seguras	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	2	3	1	1	3.3	**BAJO**

Figura 44

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A5	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades *Elaborar un procedimiento de gestión de incidentes	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	2	3	1	1	3.3	**BAJO**
	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. *Elaborar un comunicado sobre la seguridad en lugares públicos	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	1	3	1	1	1.7	**BAJO**
	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades *Elaborar un procedimiento de gestión de incidentes	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**						
	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización. *Elaborar y comunicar una política/procedimiento de Gestión de medios removibles información método cifrado	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**						
A6	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios. *Elaborar y comunicar la política de control de accesos *Elaborar y comunicar la política de escritorio y pantalla limpia	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	1	1	1	1	1.0	**BAJO**

Figura 45

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A7	Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos. *Comunicar sobre el buen uso de correo corporativo	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	1	1	2	2	1.7	**BAJO**
	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. *Elaborar y comunicar una política de transferencia de información *Comunicar sobre el buen uso de correos corporativos y el cuidado con los enlaces sospechosos	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**	1	1	2	2	1.7	**BAJO**
	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	Desarrollo de procesos/Business Partner	23/08/2021	17/09/2021	**100%**						
A8	Prevenir el acceso no autorizado a los sistemas y aplicaciones. *Verificar que los colaboradores asignados tengan los accesos al Share Point *Comunicar sobre repositorio de información	Analista Junior de Business Infelice/Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	2	1	2	1	2.7	**MEDIO**

Figura 46

Controles SI

IDENTIFICACIÓN DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
N° DE ACTIVO							D	I	C		
A9	Prevenir el acceso no autorizado a los sistemas y aplicaciones. *Verificar que los colaboradores asignados tengan los accesos al drive *Comunicar sobre repositorio de información	Analista Junior de Business Intelligence/Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	2	1	2	1	2.7	**MEDIO**
A10	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos a la plataforma de E-learning-intranet	Analista Junior de Business Intelligence /Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
A11	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos a la plataforma de Elearnin-intranet	Analista Junior de Business Intelligence/Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
A12	Prevenir el acceso no autorizado a los sistemas y aplicaciones. Verificar que solo los colaboradores tengan los accesos para el uso correcto de Outlook	Analista Junior de Business Intelligence /Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	1	1	1	3	1.7	**BAJO**
A13	Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Analista Junior de Business Intelligence /Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	1	3	1	1	1.7	**BAJO**
A18	Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.	Analista Junior de Business Intelligence /Desarrollo de procesos	24/08/2021	8/09/2021	**100%**	1	3	1	1	1.7	**BAJO**
A19	Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos *Cada colaborar que cuente con laptop, tablep deben contar con un antivirus confiable, y actualizado.	Analista Junior de Business Intelligence /Desarrollo de procesos	24/08/2021	23/09/2021	**100%**	1	1	2	2	1.7	**BAJO**

Figura 47

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO D	IMPACTO I	IMPACTO C	RIESGO RESIDUAL	NIVEL DE RIESGO
A21	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización *Elaborar un comunicado sobre la seguridad en lugares públicos y protección del equipo con contraseñas seguras	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	2	2	2	2	4.0	**MEDIO**
	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. *Se elaborará y comunica una Política de control de accesos	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**						
	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**						

Figura 48

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO D	 I	 C	RIESGO RESIDUAL	NIVEL DE RIESGO
A23	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. *Elaborar una política de Trabajo remoto	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	2	3	1	1	3.3	**MEDIO**
	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. ANTIVIRUS-NAVEGACIÓN SEGURA	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**						
	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles. *Elaborar un Plan de contingencia *Comunicar la política de dispositivos móviles	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	1	1	3	1	1.7	**BAJO**
A24	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización. *Elaborar y comunicar una política/procedimiento de Gestión de medios removibles	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	1	3	3	3	3.0	**MEDIO**
	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. *Comunicar el Plan de contingencia	Desarrollo de procesos/Business Partner	23/08/2021	22/09/2021	**100%**	2	3	1	1	3.3	**BAJO**

Figura 49

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A25	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. *Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto	Jefe administrativo/Socio Principal	24/08/2021	8/09/2021	**100%**	2	3	1	1	3.3	**MEDIO**
	Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera. *Verificar los antecedentes Penales, policiales y judiciales de todos los colaboradores *Entregar las políticas de SI *Contar con los acuerdos, contratos, entre otros documentados	Jefe administrativo/Socio Principal	23/08/2021	17/09/2021	**100%**	1	1	2	1	1.3	**BAJO**
	Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información. *Dar a conocer las responsabilidades en la inducción *Brindar capacitaciones, comunicaciones relacionadas a seguridad de la información *Elaborar y comunicar un proceso disciplinario	Jefe administrativo/Socio Principal	24/08/2021	18/09/2021	**100%**	1	1	1	2	1.3	**BAJO**
	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.	Jefe administrativo/Socio Principal	25/08/2021	19/09/2021	**100%**						

Figura 50

Controles SI

IDENTIFICACIÓN DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
N° DE ACTIVO							D	I	C		
A25	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo *Levantar las actas de devolución de activos al término del contrato *si es cambio de responsabilidades, brindar y acceso adecuado	Jefe administrativo/Socio Principal	26/08/2021	20/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
	Identificar los activos de la organización y definir responsabilidades de protección apropiadas Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización. *Elaborar el procedimiento de gestión de activos *Comunicar sobre las buenas prácticas de seguridad de información	Jefe administrativo/Socio Principal	27/08/2021	21/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo. *Elaborar y comunicar una política de trabajo remoto	Jefe administrativo/Socio Principal	28/08/2021	22/09/2021	**100%**						
	Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios. *Comunicar la política de medios removibles	Jefe administrativo/Socio Principal	29/08/2021	23/09/2021	**100%**	1	1	1	1	1.0	**BAJO**
	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.	Jefe administrativo/Socio Principal	30/08/2021	24/09/2021	**100%**						

Figura 51

Controles SI

IDENTIFICACIÓN DE ACTIVO N° DE ACTIVO	ACCIONES A TOMAR	RESPONSABLE	FECHA DE INICIO	FECHA EJECUTADA	ESTADO	PROBABILIDAD	IMPACTO			RIESGO RESIDUAL	NIVEL DE RIESGO
							D	I	C		
A25	La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización Elaborar y comunicar el plan de contingencia de SI Elaborar planes de respuesta ante emergencia (continuidad)	Jefe administrativo/Socio Principal	31/08/2021	25/09/2021	**100%**	2	2	2	3	4.7	**MEDIO**
	La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización *Actualizar el MOF *Elaborar la política de gestión de activos(con las responsabilidades del propietario del activo, custodio y propietario del riesgo) *Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto *Concientizar sobre la importancia de un Sistema de Gestión de la información *Selección y comunicación del cargo de Oficial de seguridad de la información *Concientizar sobre la seguridad de la información	Jefe administrativo/Socio Principal	1/09/2021	26/09/2021	**100%**	1	1	2	1	1.3	**BAJO**